

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference J00024960W0	FOR FURTHER ACTION see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.	
International application No. PCT/GB 98/ 02064	International filing date (day/month/year) 13/07/1998	(Earliest) Priority Date (day/month/year) 17/07/1997
Applicant ORANGE PERSONAL COMMUNICATIONS SERVICESet al.		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 3 sheets.

☒ It is also accompanied by a copy of each prior art document cited in this report.

1. ☐ Certain claims were found unsearchable (see Box I).

2. ☐ Unity of invention is lacking (see Box II).

3. ☐ The international application contains disclosure of a **nucleotide and/or amino acid sequence listing** and the international search was carried out on the basis of the sequence listing

☐ filed with the international application.

☐ furnished by the applicant separately from the international application.

☐ but not accompanied by a statement to the effect that it did not include matter going beyond the disclosure in the international application as filed.

☐ Transcribed by this Authority

4. With regard to the title, ☐ the text is approved as submitted by the applicant

☒ the text has been established by this Authority to read as follows:

ENCRYPTED BROADCAST MESSAGES IN A CELLULAR COMMUNICATIONS SYSTEM

5. With regard to the abstract,

☒ the text is approved as submitted by the applicant

☐ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this International Search Report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is:

Figure No. 1 ☒ as suggested by the applicant.

☐ None of the figures.

☐ because the applicant failed to suggest a figure.

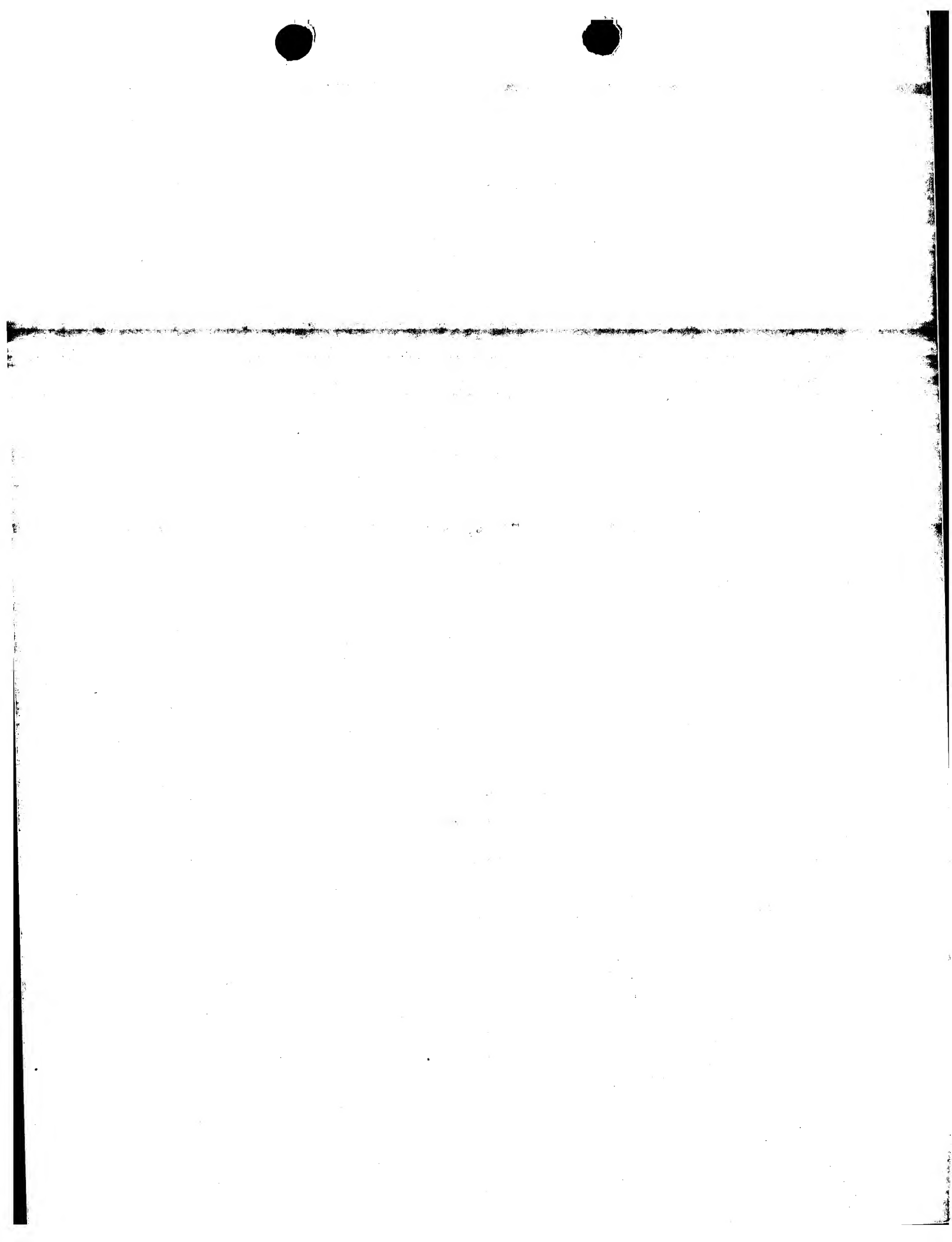
☐ because this figure better characterizes the invention.

INTERNATIONAL SEARCH REPORT

International Application No

PCT/GB 98/02064

A. CLASSIFICATION OF SUBJECT MATTER IPC 6 H0407/22 H0407/32		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) IPC 6 H04Q		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 96 41493 A (ERICSSON TELEFON AB L M) 19 December 1996	1, 2, 6, 13-16, 18-21, 25
Y	see page 40, line 5 - page 41, line 2 see page 52, line 20 - page 53, line 17 see page 55, line 10 - line 17 see page 57, line 19 - page 58, line 6 see claims 1-10 <div style="text-align: center;">--- -/--</div>	3, 7, 8, 12, 17, 22
<div style="display: flex; justify-content: space-between;"> <input checked="" type="checkbox"/> Further documents are listed in the continuation of box C. <input checked="" type="checkbox"/> Patent family members are listed in annex. </div>		
* Special categories of cited documents :		
<div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> <p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier document but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p> </div> <div style="width: 45%;"> <p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.</p> <p>"&" document member of the same patent family</p> </div> </div>		
Date of the actual completion of the international search <div style="text-align: center; font-weight: bold;">10 November 1998</div>		Date of mailing of the international search report <div style="text-align: center; font-weight: bold;">18/11/1998</div>
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016		Authorized officer <div style="text-align: center; font-weight: bold;">Baas, G</div>



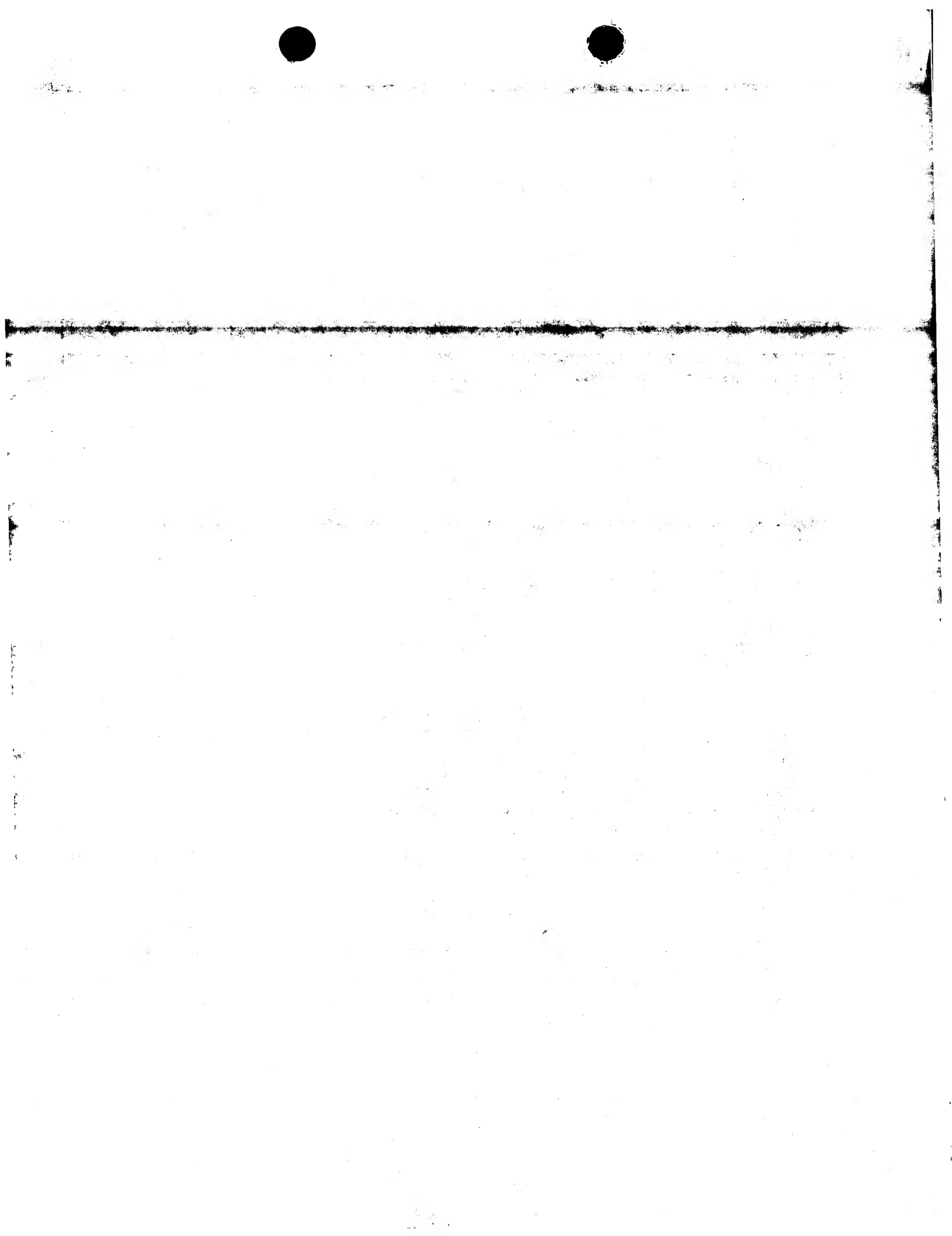
INTERNATIONAL SEARCH REPORT

International Application No

PCT/GB 98/02064

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	FARRUGIA A J ET AL: "SMART CARD TECHNOLOGY APPLIED TO THE FUTURE EUROPEAN CELLULAR TELEPHONE ON THE DIGITAL D-NETWORK" SELECTED PAPERS FROM THE SECOND INTERNATIONAL SMART CARD 2000 CONFERENCE, 4-6 OCTOBER 1989, AMSTERDAM, NL, 1 January 1989, pages 95-107, XP000472724 see page 100, line 1 - page 103, line 21 ---	3,7,8, 12,22
Y	US 5 371 493 A (SHARPE ANTHONY K ET AL) 6 December 1994 see column 3, line 3 - line 10 see column 6, line 35 - line 42 ---	17
A	EP 0 689 368 A (PTT GENERALDIREKTION) 27 December 1995 -----	



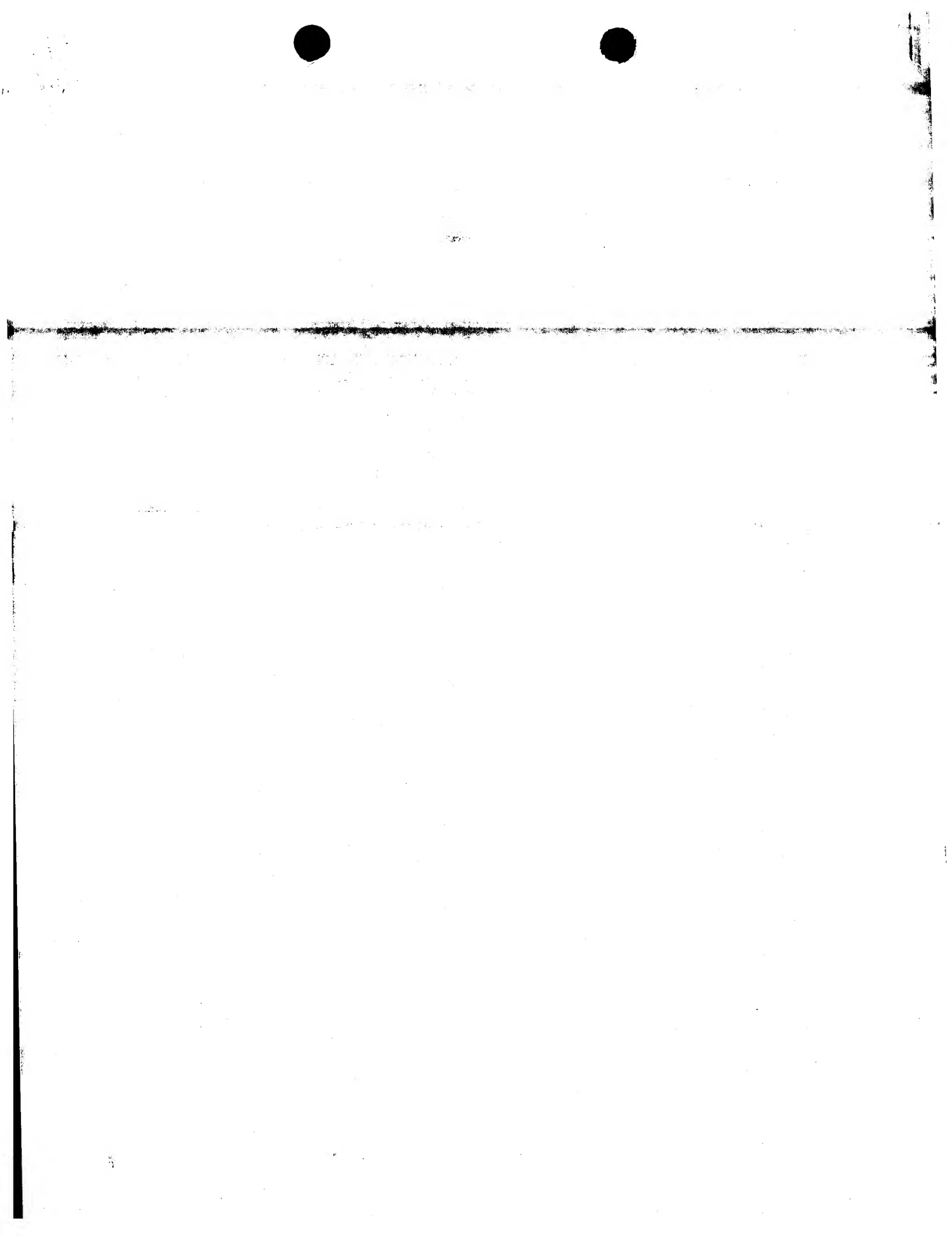
INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/GB 98/02064

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 9641493	A	19-12-1996	US 5768276 A	16-06-1998
			AU 6020296 A	30-12-1996
US 5371493	A	06-12-1994	DE 69219991 D	03-07-1997
			DE 69219991 T	27-11-1997
			EP 0538933 A	28-04-1993
			JP 5218946 A	27-08-1993
			SG 48347 A	17-04-1998
EP 0689368	A	27-12-1995	AT 153206 T	15-05-1997
			AU 691271 B	14-05-1998
			AU 2174595 A	04-01-1996
			BR 9508091 A	12-08-1997
			CA 2152215 A	21-12-1995
			WO 9535635 A	28-12-1995
			CN 1128476 A	07-08-1996
			CZ 9603513 A	14-05-1997
			DE 59402759 D	19-06-1997
			DK 689368 T	08-12-1997
			ES 2103557 T	16-09-1997
			FI 965078 A	17-12-1996
			GR 3023908 T	30-09-1997
			HU 76397 A	28-08-1997
			JP 8265843 A	11-10-1996
			NO 965315 A	18-02-1997
			NZ 287390 A	19-12-1997
			PL 317643 A	14-04-1997
			SG 34235 A	06-12-1996
			SI 9520064 A	30-04-1997
			SK 161396 A	05-11-1997
			ZA 9505091 A	10-04-1996



PATENT COOPERATION TREATY

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

United States Patent and Trademark
Office
(Box PCT)
Crystal Plaza 2
Washington, DC 20231
ÉTATS-UNIS D'AMÉRIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 06 April 1999 (06.04.99)	
International application No. PCT/GB98/02064	Applicant's or agent's file reference J00024960WO
International filing date (day/month/year) 13 July 1998 (13.07.98)	Priority date (day/month/year) 17 July 1997 (17.07.97)
Applicant FORD, Peter	

1. The designated Office is hereby notified of its election made:



in the demand filed with the International Preliminary Examining Authority on:

17 February 1999 (17.02.99)



in a notice effecting later election filed with the International Bureau on:

2. The election ☒ was

was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No.: (41-22) 740.14.35	Authorized officer Lazar Joseph Panakal Telephone No.: (41-22) 338.83.38
---	--

1

9/46346

17

PATENT COOPERATION TREATY

PCT

REC'D 15 DEC 1999	
WIPO	PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference J00024960WO		See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416) FOR FURTHER ACTION
International application No. PCT/GB98/02064	International filing date (day/month/year) 13/07/1998	Priority date (day/month/year) 17/07/1997
International Patent Classification (IPC) or national classification and IPC H04Q7/22		
Applicant ORANGE PERSONAL COMMUNICATIONS SERVICESet al.		

RECEIVED
JUN 14 2001
Group 2100


- This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
- This REPORT consists of a total of 6 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

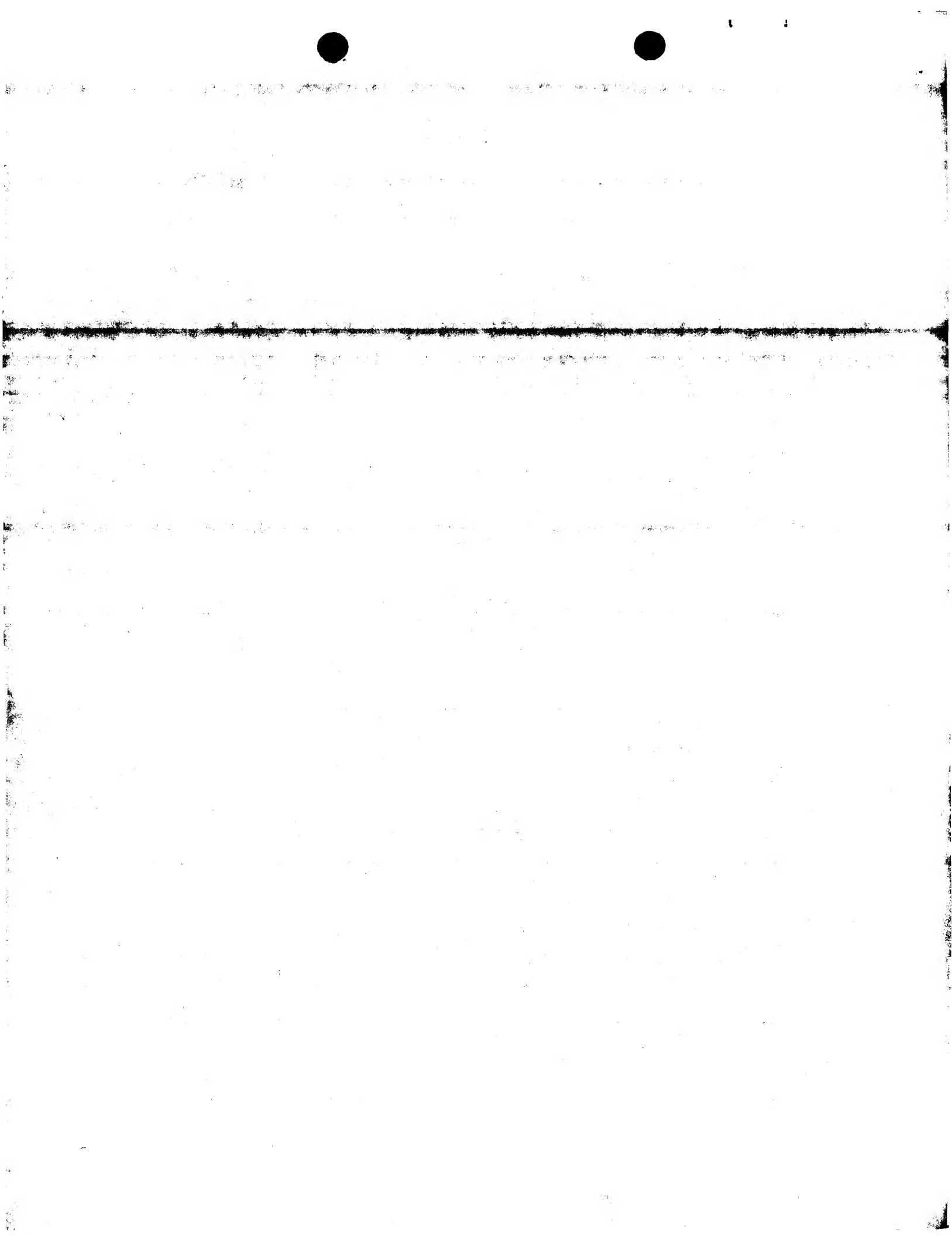
 These annexes consist of a total of 5 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☒ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand 17/02/1999	Date of completion of this report 10.12.99
Name and mailing address of the international preliminary examining authority:  European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer Hamer, J Telephone No. +49 89 2399 8827





INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference J00024960WO	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/GB98/02064	International filing date (day/month/year) 13/07/1998	Priority date (day/month/year) 17/07/1997
International Patent Classification (IPC) or national classification and IPC H04Q7/22		
Applicant ORANGE PERSONAL COMMUNICATIONS SERVICESet al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.



2. This REPORT consists of a total of 6 sheets, including this cover sheet.

- ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 5 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☒ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand 17/02/1999	Date of completion of this report 1 0. 12. 99
Name and mailing address of the international preliminary examining authority:  European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer Hamer, J Telephone No. +49 89 2399 8827 

THIS PAGE BLANK (USPTO)

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. PCT/GB98/02064

I. Basis of the report

1. This report has been drawn on the basis of (*substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

Description, pages:

1-25 as originally filed

Claims, No.:

1-18 as received on 02/07/1999 with letter of 01/07/1999

Drawings, sheets:

1/8-8/8 as originally filed

2. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
☐ the claims, Nos.:
☐ the drawings, sheets:

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

4. Additional observations, if necessary:

III. Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

The questions whether the claimed invention appears to be novel, to involve an inventive step (to be non-obvious), or to be industrially applicable have not been examined in respect of:

- ☐ the entire international application.
☒ claims Nos. 17,18.

because:

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. PCT/GB98/02064

☐ the said international application, or the said claims Nos. relate to the following subject matter which does not require an international preliminary examination (*specify*):

☒ the description, claims or drawings (*indicate particular elements below*) or said claims Nos. 17,18 are so unclear that no meaningful opinion could be formed (*specify*):

see separate sheet

☐ the claims, or said claims Nos. are so inadequately supported by the description that no meaningful opinion could be formed.

☐ no international search report has been established for the said claims Nos. .

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-16
	No:	Claims	
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-16
Industrial applicability (IA)	Yes:	Claims	1-16
	No:	Claims	

2. Citations and explanations

see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

THIS PAGE BLANK (USPTO)

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/GB98/02064

III-No Opinion

1. Independent claims 17 and 18 are not clearly expressed and do not contain any features relating to their claimed subject-matter. The claims should have been presented as dependent claims.

V- Reasoned Statement

1. The following documents are cited:

D1: WO 96 41493 A (ERICSSON TELEFON AB L M) 19 December 1996

D2: US-A-5 371 493 (SHARPE ANTHONY K ET AL) 6 December 1994

D3: EP-A-0 689 368 (PTT GENERALDIREKTION) 27 December 1995

D4: FARRUGIA A J ET AL: 'SMART CARD TECHNOLOGY APPLIED TO THE FUTURE EUROPEAN CELLULAR TELEPHONE ON THE DIGITAL D-NETWORK' SELECTED PAPERS FROM THE SECOND INTERNATIONAL SMART CARD 2000 CONFERENCE, 4-6 OCTOBER 1989, AMSTERDAM, NL, 1 January 1989, pages 95-107, XP000472724

2. The subject-matter of claim 1 is concerned with a method of distributing information to users in a cellular telecommunications network. Such a network includes base stations which transmit in cells and mobile stations which can move around freely. One service which may be provided within such a network consists of pages of text or other messages being transmitted on a common channel in one or more cell. In order to cover the cost of such a system, a subscription charge might be levied. As only those who have paid a subscription charge should be able to make use of any information transmitted, the information is encrypted before transmission. According to claim 1, the decryption key required is contained in a removable module which may be used in association with any of a plurality of mobile stations.

These features are all known from document D1 (see passages cited in the international search report) which specifies a similar method of distributing information and in which the decryption key is contained on a removable module which may be a smart card. The last feature of claim 1 is not found in D1. This

THIS PAGE BLANK (USPTO)

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. PCT/GB98/02064

I. Basis of the report

1. This report has been drawn on the basis of (*substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

Description, pages:

1-25 as originally filed

Claims, No.:

1-18 as received on 02/07/1999 with letter of 01/07/1999

Drawings, sheets:

1/8-8/8 as originally filed

RECEIVED
JUN 14 2001
Group 2100

2. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
☐ the claims, Nos.:
☐ the drawings, sheets:

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

4. Additional observations, if necessary:

III. Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

The questions whether the claimed invention appears to be novel, to involve an inventive step (to be non-obvious), or to be industrially applicable have not been examined in respect of:

- ☐ the entire international application.
☒ claims Nos. 17,18.

because:

1009847000
1009847000
1009847000

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. PCT/GB98/02064

☐ the said international application, or the said claims Nos. relate to the following subject matter which does not require an international preliminary examination (*specify*):

☒ the description, claims or drawings (*indicate particular elements below*) or said claims Nos. 17,18 are so unclear that no meaningful opinion could be formed (*specify*):

see separate sheet

☐ the claims, or said claims Nos. are so inadequately supported by the description that no meaningful opinion could be formed.

☐ no international search report has been established for the said claims Nos. .

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims 1-16
	No:	Claims
Inventive step (IS)	Yes:	Claims
	No:	Claims 1-16
Industrial applicability (IA)	Yes:	Claims 1-16
	No:	Claims

2. Citations and explanations

see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/GB98/02064

III-No Opinion

1. Independent claims 17 and 18 are not clearly expressed and do not contain any features relating to their claimed subject-matter. The claims should have been presented as dependent claims.

V- Reasoned Statement

1. The following documents are cited:

D1: WO 96 41493 A (ERICSSON TELEFON AB L M) 19 December 1996
D2: US-A-5 371 493 (SHARPE ANTHONY K ET AL) 6 December 1994
D3: EP-A-0 689 368 (PTT GENERALDIREKTION) 27 December 1995
D4: FARRUGIA A J ET AL: 'SMART CARD TECHNOLOGY APPLIED TO THE FUTURE EUROPEAN CELLULAR TELEPHONE ON THE DIGITAL D-NETWORK' SELECTED PAPERS FROM THE SECOND INTERNATIONAL SMART CARD 2000 CONFERENCE, 4-6 OCTOBER 1989, AMSTERDAM, NL, 1 January 1989, pages 95-107, XP000472724

2. The subject-matter of claim 1 is concerned with a method of distributing information to users in a cellular telecommunications network. Such a network includes base stations which transmit in cells and mobile stations which can move around freely. One service which may be provided within such a network consists of pages of text or other messages being transmitted on a common channel in one or more cell. In order to cover the cost of such a system, a subscription charge might be levied. As only those who have paid a subscription charge should be able to make use of any information transmitted, the information is encrypted before transmission. According to claim 1, the decryption key required is contained in a removable module which may be used in association with any of a plurality of mobile stations.

These features are all known from document D1 (see passages cited in the international search report) which specifies a similar method of distributing information and in which the decryption key is contained on a removable module which may be a smart card. The last feature of claim 1 is not found in D1. This

feature is that decryption takes place within the removable module.

This feature is, however, already known from document D4 in which a subscriber identity module or SIM contains not only a decryption key, but also has self contained intelligence and performs the decryption algorithms within itself. The SIM is also capable of storing the results. Attention is drawn in D4 to page 95, paragraph 4., page 97, paragraph 14., pages 100 to 102, sections A and B, pages 103 to 105, part V and sections A and B. This feature known from D4 provides the same advantages of network transparency as the method known from claim 1.

Thus a skilled person, aware of the disclosure of D1 and wishing to involve more system transparency, would need no inventive skill to add the feature known from D4 of performing decryption within the removable module, in order to arrive at the subject-matter of claim 1. As a result, claim 1 does not involve an inventive step and does not, therefore, meet the requirements of Article 33(3) PCT.

3. The subject-matter of independent claim 14 is directed towards an apparatus for receiving information. This claim contains essentially the same subject-matter as claim 1 expressed in terms of apparatus features. These features have already been discussed in the preceding paragraph with respect to method claim 1.

As a result and for the same reasons, the subject-matter of claim 14 does not meet the requirements of Article 33(3) PCT.

4. The subject-matter of the dependent claims 2 to 13 and 14 to 16 do not appear to contain features which would contribute an inventive step to the claims upon which they depend. All of the features are either obvious to a skilled person or are disclosed in the documents D1 to D4 cited in the international search report. One reason for this is that not only features relating to the transmission and reception of encrypted signals, but also to the basic idea of the application are already known.

As a result, the dependent claims also do not meet the requirements of Article 33(3) PCT.

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/GB98/02064

VII- Certain Defects

The following deficiencies are found in the application:

- a) The claims do not meet the requirements of Rule 6.2(b) PCT in that they do not contain reference signs.
- b) The independent claims do not meet the requirements of Rule 6.3(b) PCT in that they are not divided into the two-part form.
- c) The most relevant of the documents cited in the International Search Report should have been referenced and briefly discussed in the description, Rule 5.1(a)(ii), PCT.
- d) The description should have been modified to bring it into agreement with the modified independent claims, Rule 5.1(a)(iii), PCT.

CLAIMS

1. A method of distributing information to users in a cellular telecommunications network comprising a plurality of base stations transceiving
5 in a plurality of cells of said network, said method comprising:

providing a plurality of mobile stations, each of said mobile stations having an associated information access status;

broadcasting a signal on a common channel of at least one cell of said network, said signal containing a limited access message in encrypted form, for
10 general reception in said at least one cell;

enabling first mobile stations having a first information access status to decrypt and present said message to a user in unencrypted form when being served by said cell; and

preventing second mobile stations having a second information access
15 status from presenting said message in unencrypted form to a user when being served in said cell,

wherein said first mobile stations are provided with a removable module which may be used in association with any of a plurality of mobile stations, said removable module storing a decryption key for said message,

20 and wherein said message is decrypted, using said decryption key, in said removable module.

2. A method according to claim 1, wherein said signal comprises a message identifier accompanying a message and said method comprises enabling both said first and second mobile stations to read said message identifier.

5

3. A method according to claim 1 or 2, wherein said decryption key is stored in said removable module in encrypted form.

10

4. A method according to claim 3, wherein said decryption key is decrypted by said first mobile station using a data string specific to said removable module.

15

5. A method according to claim 4, wherein said data string is a subscriber identifier used in said cellular telecommunications network.

6. A method according to any preceding claim, further comprising transmitting said decryption key to said first mobile stations via a radio interface in said cellular telecommunications network.

20

7. A method according to any preceding claim, wherein said removable module is a subscriber identity module.

AMENDED SHEET



8. A method according to claim 7, wherein said message includes a transfer protocol identifier indicating that the message is of a type for data download to the subscriber identity module from the mobile station.

5 9. A method according to any preceding claim, wherein said removable module stores an application programme for performing the decryption and for controlling a display of said message on the mobile station.

10 10. A method according to any preceding claim, wherein said signal comprises a plurality of limited access messages each having a corresponding decryption key,

said method comprising providing said first mobile stations with said decryption keys, storing said decryption keys on removable modules of said first mobile stations, and enabling only ones of said first mobile stations having
15 a decryption key corresponding to a limited access message to present said limited access message to a user in unencrypted form when being served in said cell.

20 11. A method according to claim 10, comprising providing each of said first mobile stations with a selection of said subscription keys in accordance with a subscription held for each first mobile station respectively.

AMENDED SHEET

THIS PAGE BLANK (USPTO)

29

12. A method according to any preceding claim, wherein alternative limited access messages are broadcast in cells located in different areas of said cellular telecommunications network.

5 13. A method according to any preceding, wherein said common channel is a cell broadcast channel of a GSM-type communications system.

14. A mobile station for receiving information in a cellular telecommunications system, said mobile station comprising:

10 means for receiving an encrypted message broadcast on a common channel of a cell of said cellular telecommunications system; and

means for displaying said message, when decrypted, to a user; and

a removable module comprising a memory for storing a decryption key, and means for decrypting said message using said stored decryption key.

15

15. A mobile station according to claim 14, wherein said removable module is a subscriber identity module.

16. A mobile station according to claim 14 or 15, wherein said

20 removable module stores an application programme for performing the decryption and for controlling the display of said message on the mobile station.

AMENDED SHEET

THIS PAGE BLANK (USPTO)

17. A GSM Phase 2+ mobile station according to any of claims 14 to 16.

5 18. A cellular mobile telephone according to any of claims 14 to 17.

AMENDED SHEET

THIS PAGE BLANK (USPTO)

PATENT COOPERATION TREATY

PCT

REC'D 18 OCT 1999

WIPO PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference J00024960WO		FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/GB98/02064	International filing date (day/month/year) 13/07/1998	Priority date (day/month/year) 17/07/1997	
International Patent Classification (IPC) or national classification and IPC H04Q7/22			
Applicant ORANGE PERSONAL COMMUNICATIONS SERVICESet al.			



1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 6 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 5 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☒ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand 17/02/1999	Date of completion of this report 13. 10. 99
Name and mailing address of the international preliminary examining authority:  European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer Hamer, J Telephone No. +49 89 2399 8827 

THIS PAGE BLANK (USPTO)

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. PCT/GB98/02064

I. Basis of the report

1. This report has been drawn on the basis of (*substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

Description, pages:

1-25 as originally filed

Claims, No.:

1-18 as received on 02/07/1999 with letter of 01/07/1999

Drawings, sheets:

1/8-8/8 as originally filed

2. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
☐ the claims, Nos.:
☐ the drawings, sheets:

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

4. Additional observations, if necessary:

III. Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

The questions whether the claimed invention appears to be novel, to involve an inventive step (to be non-obvious), or to be industrially applicable have not been examined in respect of:

- ☐ the entire international application.
☒ claims Nos. 17,18.

because:

THIS PAGE BLANK (USPTO)

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. PCT/GB98/02064

☐ the said international application, or the said claims Nos. relate to the following subject matter which does not require an international preliminary examination (*specify*):

☒ the description, claims or drawings (*indicate particular elements below*) or said claims Nos. 17,18 are so unclear that no meaningful opinion could be formed (*specify*):

see separate sheet

☐ the claims, or said claims Nos. are so inadequately supported by the description that no meaningful opinion could be formed.

☐ no international search report has been established for the said claims Nos. .

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-16
	No:	Claims	
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-16
Industrial applicability (IA)	Yes:	Claims	1-16
	No:	Claims	

2. Citations and explanations

see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

THIS PAGE BLANK (USPTO)

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/GB98/02064

III-No Opinion

1. Independent claims 17 and 18 are not clearly expressed and do not contain any features relating to their claimed subject-matter. The claims should have been presented as dependent claims.

V- Reasoned Statement

1. The following documents are cited:

D1: WO 96 41493 A (ERICSSON TELEFON AB L M) 19 December 1996
D2: US-A-5 371 493 (SHARPE ANTHONY K ET AL) 6 December 1994
D3: EP-A-0 689 368 (PTT GENERALDIREKTION) 27 December 1995
D4: FARRUGIA A J ET AL: 'SMART CARD TECHNOLOGY APPLIED TO THE FUTURE EUROPEAN CELLULAR TELEPHONE ON THE DIGITAL D-NETWORK' SELECTED PAPERS FROM THE SECOND INTERNATIONAL SMART CARD 2000 CONFERENCE, 4-6 OCTOBER 1989, AMSTERDAM, NL, 1 January 1989, pages 95-107, XP000472724

2. The subject-matter of claim 1 is concerned with a method of distributing information to users in a cellular telecommunications network. Such a network includes base stations which transmit in cells and mobile stations which can move around freely. One service which may be provided within such a network consists of pages of text or other messages being transmitted on a common channel in one or more cell. In order to cover the cost of such a system, a subscription charge might be levied. As only those who have paid a subscription charge should be able to make use of any information transmitted, the information is encrypted before transmission. According to claim 1, the decryption key required is contained in a removable module which may be used in association with any of a plurality of mobile stations.

These features are all known from document D1 (see passages cited in the international search report) which specifies a similar method of distributing information and in which the decryption key is contained on a removable module which may be a smart card. The last feature of claim 1 is not found in D1. This

THIS PAGE BLANK (USPTO)

feature is that decryption takes place within the removable module.

This feature is, however, already known from document D2 in which a subscriber identity module or SIM contains not only a decryption key, but also has self contained intelligence and performs the decryption algorithms within itself. The SIM is also capable of storing the results. Attention is drawn in D2 to page 94, paragraph 4., page 97, paragraph 14., pages 100 to 102, sections A and B, pages 103 to 105, part V and sections A and B. This feature known from D2 provides the same advantages of network transparency as the method known from claim 1.

Thus a skilled person, aware of the disclosure of D1 and wishing to involve more system transparency, would need no inventive skill to add the feature known from D2 of performing decryption within the removable module, in order to arrive at the subject-matter of claim 1. As a result, claim 1 does not involve an inventive step and does not, therefore, meet the requirements of Article 33(3) PCT.

3. The subject-matter of independent claim 14 is directed towards an apparatus for receiving information. This claim contains essentially the same subject-matter as claim 1 expressed in terms of apparatus features. These features have already been discussed in the preceding paragraph with respect to method claim 1.

As a result and for the same reasons, the subject-matter of claim 14 does not meet the requirements of Article 33(3) PCT.

4. The subject-matter of the dependent claims 2 to 13 and 14 to 16 do not appear to contain features which would contribute an inventive step to the claims upon which they depend. All of the features are either obvious to a skilled person or are disclosed in the documents D1 to D4 cited in the international search report. One reason for this is that not only features relating to the transmission and reception of encrypted signals, but also to the basic idea of the application are already known.

As a result, the dependent claims also do not meet the requirements of Article 33(3) PCT.

THIS PAGE BLANK

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/GB98/02064

VII- Certain Defects

The following deficiencies are found in the application:

- a) The claims do not meet the requirements of Rule 6.2(b) PCT in that they do not contain reference signs.
- b) The independent claims do not meet the requirements of Rule 6.3(b) PCT in that they are not divided into the two-part form.
- c) The most relevant of the documents cited in the International Search Report should have been referenced and briefly discussed in the description, Rule 5.1(a)(ii), PCT.
- d) The description should have been modified to bring it into agreement with the modified independent claims, Rule 5.1(a)(iii), PCT.

THIS PAGE BLANK (USPTO)

feature is that decryption takes place within the removable module.

This feature is, however, already known from document D4 in which a subscriber identity module or SIM contains not only a decryption key, but also has self contained intelligence and performs the decryption algorithms within itself. The SIM is also capable of storing the results. Attention is drawn in D4 to page 95, paragraph 4., page 97, paragraph 14., pages 100 to 102, sections A and B, pages 103 to 105, part V and sections A and B. This feature known from D4 provides the same advantages of network transparency as the method known from claim 1.

Thus a skilled person, aware of the disclosure of D1 and wishing to involve more system transparency, would need no inventive skill to add the feature known from D4 of performing decryption within the removable module, in order to arrive at the subject-matter of claim 1. As a result, claim 1 does not involve an inventive step and does not, therefore, meet the requirements of Article 33(3) PCT.

3. The subject-matter of independent claim 14 is directed towards an apparatus for receiving information. This claim contains essentially the same subject-matter as claim 1 expressed in terms of apparatus features. These features have already been discussed in the preceding paragraph with respect to method claim 1.

As a result and for the same reasons, the subject-matter of claim 14 does not meet the requirements of Article 33(3) PCT.

4. The subject-matter of the dependent claims 2 to 13 and 14 to 16 do not appear to contain features which would contribute an inventive step to the claims upon which they depend. All of the features are either obvious to a skilled person or are disclosed in the documents D1 to D4 cited in the international search report. One reason for this is that not only features relating to the transmission and reception of encrypted signals, but also to the basic idea of the application are already known.

As a result, the dependent claims also do not meet the requirements of Article 33(3) PCT.

THIS PAGE BLANK (USPTO)

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/GB98/02064

VII- Certain Defects

The following deficiencies are found in the application:

- a) The claims do not meet the requirements of Rule 6.2(b) PCT in that they do not contain reference signs.
- b) The independent claims do not meet the requirements of Rule 6.3(b) PCT in that they are not divided into the two-part form.
- c) The most relevant of the documents cited in the International Search Report should have been referenced and briefly discussed in the description, Rule 5.1(a)(ii), PCT.
- d) The description should have been modified to bring it into agreement with the modified independent claims, Rule 5.1(a)(iii), PCT.

THIS PAGE BLANK (USPTO)

CLAIMS

1. A method of distributing information to users in a cellular telecommunications network comprising a plurality of base stations transceiving
5 in a plurality of cells of said network, said method comprising:

 providing a plurality of mobile stations, each of said mobile stations having an associated information access status;

 broadcasting a signal on a common channel of at least one cell of said network, said signal containing a limited access message in encrypted form, for
10 general reception in said at least one cell;

 enabling first mobile stations having a first information access status to decrypt and present said message to a user in unencrypted form when being served by said cell; and

 preventing second mobile stations having a second information access
15 status from presenting said message in unencrypted form to a user when being served in said cell,

 wherein said first mobile stations are provided with a removable module which may be used in association with any of a plurality of mobile stations, said removable module storing a decryption key for said message,

20 and wherein said message is decrypted, using said decryption key, in said removable module.

THIS PAGE BLANK (USPTO)

2. A method according to claim 1, wherein said signal comprises a message identifier accompanying a message and said method comprises enabling both said first and second mobile stations to read said message identifier.

5

3. A method according to claim 1 or 2, wherein said decryption key is stored in said removable module in encrypted form.

10

4. A method according to claim 3, wherein said decryption key is decrypted by said first mobile station using a data string specific to said removable module.

15

5. A method according to claim 4, wherein said data string is a subscriber identifier used in said cellular telecommunications network.

20

6. A method according to any preceding claim, further comprising transmitting said decryption key to said first mobile stations via a radio interface in said cellular telecommunications network.

7. A method according to any preceding claim, wherein said removable module is a subscriber identity module.

AMENDED SHEET

THIS PAGE BLANK (USPTO)

8. A method according to claim 7, wherein said message includes a transfer protocol identifier indicating that the message is of a type for data download to the subscriber identity module from the mobile station.

5 9. A method according to any preceding claim, wherein said removable module stores an application programme for performing the decryption and for controlling a display of said message on the mobile station.

10 10. A method according to any preceding claim, wherein said signal comprises a plurality of limited access messages each having a corresponding decryption key.

said method comprising providing said first mobile stations with said decryption keys, storing said decryption keys on removable modules of said first mobile stations, and enabling only ones of said first mobile stations having
15 a decryption key corresponding to a limited access message to present said limited access message to a user in unencrypted form when being served in said cell.

20 11. A method according to claim 10, comprising providing each of said first mobile stations with a selection of said subscription keys in accordance with a subscription held for each first mobile station respectively.

AMENDED SHEET

THIS PAGE BLANK (USPTO)

12. A method according to any preceding claim, wherein alternative limited access messages are broadcast in cells located in different areas of said cellular telecommunications network.

5 13. A method according to any preceding, wherein said common channel is a cell broadcast channel of a GSM-type communications system.

14. A mobile station for receiving information in a cellular telecommunications system, said mobile station comprising:

10 means for receiving an encrypted message broadcast on a common channel of a cell of said cellular telecommunications system; and

means for displaying said message, when decrypted, to a user; and

a removable module comprising a memory for storing a decryption key, and means for decrypting said message using said stored decryption key.

15 15. A mobile station according to claim 14, wherein said removable module is a subscriber identity module.

16. A mobile station according to claim 14 or 15, wherein said
20 removable module stores an application programme for performing the decryption and for controlling the display of said message on the mobile station.

AMENDED SHEET

THIS PAGE BLANK (USPTO)

17. A GSM Phase 2+ mobile station according to any of claims 14 to 16.

5

18. A cellular mobile telephone according to any of claims 14 to 17.

AMENDED SHEET

THIS PAGE BLANK (USPTO)

CLAIMS

1. A method of distributing information to users in a cellular telecommunications network comprising a mobile switching centre and a plurality of base stations transceiving in a plurality of cells of said network, said method comprising:

providing a plurality of mobile stations, each of said mobile stations having an associated information access status;

broadcasting a signal on a common channel of at least one cell of said network, said signal containing a limited access message in encrypted form, for general reception in said at least one cell;

enabling first mobile stations having a first information access status to decrypt and present said message to a user in unencrypted form when being served by said cell; and

preventing second mobile stations having a second information access status from presenting said message in unencrypted form to a user when being served in said cell.

2. A method according to claim 1, wherein said first mobile stations are provided with a decryption key for said message.

THIS PAGE BLANK (USPTO)

3. A method according to claim 2, wherein said decryption key is held in a removable module which may be used in association with any of a plurality of mobile stations.

5 4. A method according to claim 3, wherein said message is decrypted in said removable module.

5. A method according to claim 2 or 3, wherein said signal contains padding data accompanying a portion of said message, and said portion is
10 contained in said signal in unencrypted form.

6. A method according to any preceding claim, wherein said signal comprises a header portion containing a message identifier accompanying a message and said method comprises enabling both said first and second mobile
15 stations to read said message identifier.

7. A method according to any of the preceding claims, wherein status data defining said information access status is stored in a removable module of a first mobile station.

20

8. A method according to claim 7, wherein said status data comprises a decryption key.

THIS PAGE BLANK (USPTO)

9. A method according to claim 8, wherein said decryption key is stored in said removable data store in encrypted form.

5 10. A method according to claim 9, wherein said decryption key is decrypted by said first mobile station using a data string specific to said removable module.

10 11. A method according to claim 10, wherein said data string is a subscriber identifier used in said cellular telecommunications network.

12. A method according to any of claims 7 to 11, further comprising transmitting said status data to said first mobile station via a radio interface in said cellular telecommunications network.

15

13. A method according to any preceding claim, wherein said signal comprises a plurality of limited access messages each having a corresponding access right,

said method comprising providing said mobile stations with said access rights and enabling only mobile stations having an access right corresponding to a limited access message to present said limited access message to a user when being served in said cell.

20

THIS PAGE BLANK (USPTO)

14. A method according to claim 13, comprising providing each of said first mobile stations with a selection of said access rights in accordance with a subscription held for each first mobile station respectively.

5

15. A method according to claim 13 or 14, further comprising storing encryption keys for each of a plurality of limited access message types, and encrypting each said limited access message using an encryption key in accordance with its respective message type.

10

16. A method according to any of claims 13 to 15, comprising storing a plurality of subscription records, each said subscription record comprising access right data defining said access rights.

15

17. A method according to claim 16, comprising altering said access right data for a subscription record to alter the type of limited access messages a user is able to receive intelligibly.

20

18. A method according to any preceding claim, wherein said signal contains a general access message, and wherein said method comprises enabling both said first and second mobile stations to present said general access message to a user when being served in said call.

THIS PAGE BLANK (USPTO)

19. A method according to claim 19, wherein said common channel is a cell broadcast channel of a GSM-type communications system.

5 20. A method according to any preceding claim, wherein alternative limited access message(s) are broadcast in cells located in different areas of said cellular telecommunications network.

21. Apparatus for receiving information in a cellular
10 telecommunicationssystem, said apparatus comprising:

means for storing a decryption key;

means for receiving a message broadcast on a common channel of a cell
of said cellular telecommunicationssystem; and

means for decrypting said message using said stored decryption key; and

15 means for displaying said decrypted message to a user.

22. Apparatus according to claim 21, wherein said storage means is part of a removable module.

20 23. Apparatus according to claim 21 or 22, wherein said displaying means is arranged to display a message in decrypted form when a decryption key for said message is held in said storage means, and to display said message

THIS PAGE BLANK (USPTO)

THIS PAGE BLANK (USPTO)

in encrypted form when no decryption key for said message is held in said storage means.

24. Apparatus according to claim 21, 22 or 23, wherein said
5 decryption means is part of a removable module.

25. A cellular mobile telephone according to claim 21, 22, 23 or 24.



(12) **EUROPÄISCHE PATENTANMELDUNG**

②¹ Anmeldenummer: 94810363.5

⑤ Int. Cl.⁶: **H04Q** 7/22

②② Anmeldetag: 20.06.94

④ Veröffentlichungstag der Anmeldung:
27.12.95 Patentblatt 95/52

Ⓔ Benannte Vertragsstaaten:
AT BE CH DE DK ES FR GB GR IE IT LI LU MC
NL PT SE

71 Anmelder: **Generaldirektion PTT**
Viktoriastrasse 21
CH-3030 Bern (CH)

(72) Erfinder: Ritter, Rudolf
Rossweidweg 8
CH-3052 Zollikofen (CH)
Erfinder: Hertel, Joachim
Theodor-Heuss-Ring 52
D-63128 Dietzenbach (DE)

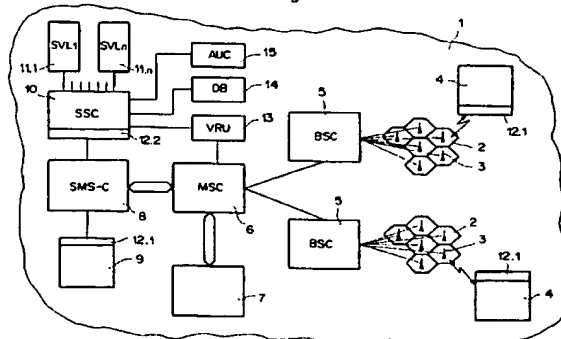
74 Vertreter: Tschudi, Lorenz et al
Bovard AG
Patentanwälte VSP
Optingenstrasse 16
CH-3000 Bern 25 (CH)

54 **Vorrichtung zur Übermittlung von Meldungen in einem mobilen Kommunikationsnetz**

57) Die Vorrichtung zur Übermittlung von Meldungen wird in einem Mobilfunknetz (1) mit einer Vielzahl von Endgeräten (4, 9) eingesetzt. Die Endgeräte können einem bestimmten Benutzer entweder fest zugeordnet sein oder mittels einer in das Endgerät einsetzbaren Chipkarte einem bestimmten Benutzer zugeordnet werden. Mindestens zwei Endgeräte können im Mobilfunknetz miteinander in eine Sprach- oder Datenkommunikation treten. Das Mobilfunknetz umfasst mindestens eine Zentrale (8) zum Steuern der Meldungsübermittlung, wobei jede Meldung eine Datenkommunikation ist, bei welcher Datentelegramme ausgetauscht werden, in welchen ein standardisierter Datenvorsatz enthalten ist. Zum Verarbeiten von besonderen Diensten nach einer speziellen Prozedur, die nur bestimmten, dazu autorisierten Teilnehmern zugänglich ist, umfasst das Datentelegramm zusätzlich zum standardisierten Datenvorsatz einen Kennungscode. Eine zentrale Einheit (10), die der Zentrale (8) zugeordnet ist und mindestens ein Teil der Endgeräte (4, 9) weisen Mittel zum Erzeugen von mit dem Kennungscode versehenen Datentelegrammen auf. Die zentrale Einheit für die besonderen Dienste sowie dazu autorisierte Endgeräte oder autorisierte Chipkarten sind mit einem

vorzugsweise softwaremässig ausgeführten Filter (12.1, 12.2) zum Erkennen des Kennungscodes ausgerüstet. Dadurch bietet sich die Möglichkeit, nicht nur beliebige Bitströme im transparenten Modus nach GSM Phase 2 zu übertragen, sondern, Daten und ausführbare Instruktionen an autorisierte Teilnehmer zu senden oder von diesen zu empfangen. Dies, ohne dass international festgelegte Standards geändert werden müssen.

Fig. 2



Die vorliegende Erfindung betrifft eine Vorrichtung zur Übermittlung von Meldungen in einem Kommunikationsnetz zur Sprach- und Datenverarbeitung mit einer Vielzahl von Endgeräten, welche einem bestimmten Benutzer zugeordnet sind, oder mittels einem in das Endgerät einsetzbaren Datenträger einem bestimmten Benutzer zugeordnet werden können, wobei mindestens zwei Endgeräte miteinander in eine Sprach- oder Datenkommunikation treten können, sowie mit mindestens einer Zentrale zum Steuern der Meldungsübermittlung innerhalb dem Kommunikationsnetz, wobei jede Meldungsübermittlung eine Datenkommunikation ist bei welcher Datentelegramme ausgetauscht werden in welchen ein standardisierter Datenvorsatz enthalten ist.

Gegenwärtig bieten viele Länder nationale Mobilfunknetze an, die eine Vielzahl technischer Standards verwenden. Für den grenzüberschreitenden Verkehr bilden die unterschiedlichen Netze jedoch ein Hindernis. Ein Mobilfunkteilnehmer erwartet, dass er sein Endgerät an verschiedenen Orten in mehreren Ländern, beispielsweise in ganz Europa verwenden kann.

Mit der Einführung des GSM-Standards (Global System for Mobil Communication), Bezeichnung für den Standard eines zellularen Mobilfunknetzes, ist der Weg zum einheitlichen Netz und somit zum grenzüberschreitenden Verkehr frei geworden.

In der Fig. 1 ist der prinzipielle Aufbau eines Mobilfunknetzes, das nach dem GSM-Standard arbeitet, gezeigt. Mit 1 sei darin der flächenmässige Bereich des Mobilfunknetzes bezeichnet. Die ganze Fläche dieses Netzes ist dabei von aneinander angrenzenden und einander überlappenden Funkzellen 2, von denen in der Fig. 1 lediglich einige wenige sichtbar sind, überdeckt. In jeder Funkzelle 2 ist eine Basisstation 3 (RBS, Radio-Base-Station) vorhanden, welche die Funkversorgung zu den Endgeräten bei den Mobilfunkteilnehmern übernehmen. Auf jeder Funkstrecke zwischen einer Basisstation 3 und einem Endgerät 4 werden alle Sprach- und Steuerinformationen sowie andere Daten wie beispielsweise Meldungen digital verschlüsselt übertragen.

Mit 5 ist ein Controller gezeichnet (BSC, Base-Station-Controller), mit dem mehrere Basisstationen gesteuert werden. Beispielsweise ist der Controller dafür verantwortlich, dass der Übergang eines Teilnehmers bzw. des dem Teilnehmer zugeordneten Endgerätes, insbesondere ein Mobilfunktelefon, von einer Funkzelle zu einer anderen benachbarten Funkzelle funktechnische reibungslos ablaufen kann. Anhand von automatisch durchgeführten Feldstärkemessungen entscheidet der Controller, wann der Übergang von einer Funkzelle zu welcher benachbarten Funkzelle eingeleitet werden soll. Ein derartiger Übergang wird Handover genannt.

Die Controller sind ihrerseits zu einer übergeordneten Mobilfunkzentrale 6 (MSC, Mobil-Service-Switching-Center) zusammengefasst, welche Zentrale den Übergang zu einem drahtgebundenen Netz 7, beispielsweise einem ISDN-Netz (ISDN, Integrated Services Digital Network), also einem digitalen dienstintegrierten Fernmeldenetz, herstellt. Auf einem solchen Fernmeldenetz können beispielsweise gleichzeitig Sprachinformationen, Bildinformationen, Informationen von EDV-Anlagen, etc. übertragen werden.

Mit 9 ist ein weiteres Endgerät, beispielsweise ein Personal Computer (PC), gezeigt, mit welchem unter anderem als Anwendung einer Datenkommunikation Meldungen zu einem Mobilfunktelefon 4 übertragen werden können. Die Möglichkeit, dies zu tun, ist in der Fachwelt unter einem mit SMS (SMS, Short Message Service) benannten Dienst bekannt. Meldungen können jedoch auch von einem Mobilfunktelefon zu einem anderen Mobilfunktelefon übermittelt werden. Die Verbindung wird dabei stets über eine Zentrale für den Kurzmeldungsdienst 8, ein sogenanntes Short Message Service Center 8 (SMS-C), abgewickelt. Der Dienst SMS zur Übermittlung von Kurzmeldungen ist ein Telekommunikationsdienst der es erlaubt, Nachrichten von dem Short Message Service Center an einen GSM-Teilnehmer zu schicken (SMS MT/PP, Mobile Terminated / Point-to-Point) bzw. diese von einem GSM-Teilnehmer an den Short Message Service Center (SMS MO/PP, Mobile Originated / Point-to-Point) zu übermitteln. Jede Meldung ist dabei in einem Datentelegramm verpackt, welchem ein Datenvorsatz, ein standardisierter Header, vorgespannt ist, in welchem u.a. die Identifikation des Teilnehmers und ein Code, dass es sich hier um eine Meldung handelt, enthalten ist.

Mit GSM Phase 2 ist dieses Vorgehen, das im Standard GSM 3.40 definiert ist, bezeichnet. Es erlaubt, beliebige Bitströme in einem transparenten Modus zu übertragen. Kurzmeldungen wie beispielsweise "Ruf doch bitte den Teilnehmer xyz an" lassen sich damit von einem Teilnehmer A über den Short Message Service Center an einen Teilnehmer B übermitteln. Die Meldung wird beim Empfänger beispielsweise auf einem Display angezeigt.

Ab GSM Phase 2 gibt es auch die sogenannte Klasse 2 Nachrichten. Bei Mobilfunktelefonen oder anderen Endgeräten, die zum Verarbeiten von Klasse 2 Nachrichten vorgesehen sind, wird dabei vorausgesetzt, dass ein Speichermittel vorhanden ist, vorzugsweise ein Teilnehmer-Identifikations-Modul (SIM, Subscriber Identification Module) in der Ausbildung einer Chipkarte. Im Speichermittel sind unter anderem alle für die Identifikation des Benützers notwendigen Daten enthalten. Chipkarten oder Prozessorchipkarten sind in ein beliebiges zu ver-

wendendes Endgerät einsetzbar. Ein Vorteil einer solchen Ausführung liegt darin, dass beispielsweise ein Mobilfunkteilnehmer nicht sein persönliches Endgerät bei sich tragen muss, sondern lediglich seine Chipkarte.

Die Nachrichten der Klasse 2 oder darauf basierender Weiterentwicklungen, welche aus einer oder mehreren Meldungen bestehen können, werden meldungsweise auf dem vorgenannten Speichermittel abgelegt. Sobald dies geschehen ist wird eine positive Empfangsbestätigung an den Short Message Service Center gesendet.

Damit bietet sich die Möglichkeit, sowohl Daten als auch ausführbare Instruktionen an ein Speichermittel in einem Endgerät zu senden oder von diesem zu empfangen.

Die Aufgabe der vorliegenden Erfindung war es somit, die vorteilhaften Eigenschaften der Klasse 2 Nachrichten weiter auszubauen und mit dem SMS Dienst nicht lediglich transparente Bitströme zu übermitteln, sondern besondere Dienste an dazu autorisierte Teilnehmer anzubieten.

Erfindungsgemäss ist dies mit einer Vorrichtung zur Übermittlung von Meldungen in einem Kommunikationsnetz zur Sprach- und Datenverarbeitung gelöst worden, die die im kennzeichnenden Teil des Patentanspruches 1 aufgeführten Merkmale aufweist.

Mit dem erfindungsgemässen Kennungscode, der zusätzlich zum standardisierten Datenvorsatz oder Header in einem Datentelegramm einer Meldung vorhanden sein kann, wird gekennzeichnet, dass die in dieser Meldung vorhandenen Daten Daten sind, die nach einer speziellen Prozedur zu verarbeiten sind. Der Kennungscode, der vorteilhafterweise anschliessend an den standardisierten Datenvorsatz oder Header vorhanden ist, wird entweder von einer zentralen Einheit oder von Endgeräten, die dazu ausgerüstet sind, erzeugt und zusammen mit dem Datentelegramm der Gegenstelle, entweder dem Endgerät oder der zentralen Einheit, übermittelt. Sowohl die zentrale Einheit als auch Endgeräte, die dazu ausgerüstet sind, prüfen beim Empfang eines jeden Datentelegrammes, welches am standardisierten Datenvorsatz erkennbar ist, ob die Meldung zusätzlich einen Kennungscode enthält. Ist dies nicht der Fall, werden die Daten des Datentelegrammes als normale, bisher übliche Meldung gemäss SMS-Standard behandelt. Ist dies der Fall, weiss die zentrale Einheit, dass der Absender des Telegrammes Informationen sendet, die einem besonderen, sonst nicht zugänglichen Dienst oder einer besonderen Anwendung zuzuordnen sind. Ebenfalls weiss in diesem Falle das Endgerät, dass die im Telegramm mit einem erkannten Kennungscode vorhandenen Daten Daten zum Bearbeiten und/oder Anzeigen von Informationen eines bestimmten vorgängig angewählten besonderen

Dienstes umfassen. Mit dem Kennungscode ausgerüstete Datentelegramme ermöglichen, Daten und ausführbare Instruktionen an speziell mit einem Filter zum Erkennen solcher Datentelegramme ausgerüstete Endgeräte zu übertragen bzw. von solchen Endgeräten in der zentralen Einheit, die ebenfalls ein entsprechendes Filter umfasst, zu empfangen. Davon ausgehend lässt sich zwischen den entsprechend ausgerüsteten Endgeräten und der zentralen Einheit, welche eine steuernde Zentrale, ein sogenannter Service Center ist, ein Anwendungsprotokoll definieren, das für das angesteuerte Endgerät die Nachrichtensynchronisation, Datenauthentizität mittels Kryptogramm und Generierung einer ausführbaren Instruktion regelt. Auf der Basis des Anwendungsprotokolls können neue vom Netzbetreiber dem entsprechenden Teilnehmer offerierte Dienste definiert werden, die sich als Nachrichtenaustausch zwischen einem mit einem entsprechenden Filter versehenen Endgerät und dem Service Center verstehen lassen. Als Beispiel eines solchen besonderen Dienstes ist es beispielsweise möglich, ortsabhängige Abfragen durchzuführen. So kann unter anderem ermöglicht werden, ortsabhängige Telefonnummern von Hilfsdiensten, wie Pannendienst, Arzt, Apotheke etc., abzufragen.

Der Kennungscode kann vom Netzbetreiber festgelegt werden. Er braucht auf keine internationalen Standards abgestimmt zu sein und er kann beliebig entwickelte Sicherheitseinrichtungen umfassen, derart, dass eine zufällige Inanspruchnahme von besonderen Diensten durch nicht berechtigte Teilnehmer ausgeschlossen werden kann. Das Filter ist zweckmässigerweise als Softwaremodul aufgebaut. Dieses Softwaremodul muss zur Zeit des Festlegens der Initialdaten in einem Endgerät, welches einem Teilnehmer fest zugeordnet wird oder auf einem Datenträger, vorzugsweise auf einer Chipkarte, welcher einem Teilnehmer fest zugeordnet wird und in einer Vielzahl von nicht zugeordneten Endgeräten einsetzbar ist, gespeichert werden.

Da das genannte Kommunikationsnetz, in dem die Vorrichtung zur Anwendung gelangt, vorzugsweise ein digital arbeitendes Kommunikationsnetz ist, insbesondere jedoch ein zellular aufgebautes Mobilfunknetz, das nach dem GSM Standard oder dem DCS 1800 Standard definiert ist, sind als Endgeräte überwiegend Mobilfunktelefone vorgesehen. Diese sind zunehmend derart ausgerüstet, dass sie eine Schreib-Lese-Vorrichtung für eine Chipkarte, insbesondere für Prozessorchipkarten (SIM Subscriber-Identification-Modul) enthalten. Ein Endgerät könnte aber auch ein Datenverarbeitungsgerät, wie beispielsweise ein Personalcomputer oder ein Handheldcomputer sein. Es wäre aber ebenfalls denkbar, dass solche Geräte, obschon bis heute noch nicht üblich, in Zukunft ebenfalls

eine Datenschreib-Lese-Vorrichtung für Chipkarten aufweisen könnten. Benutzerspezifische EDV-Daten sind ja bereits heute mittels mobilen Datenträgern wie Disketten, Festplatten oder Speichermittel, nach dem PCMCIA-Standard in Chipkartengrösse an verschiedenen EDV-Geräten einsetzbar.

Flussdiagrammmässig stellt das genannte Filter eine Verzweigungseinrichtung dar, welche Meldungen, die den Kennungscode nicht enthalten, an einen ersten Ausgang weitergibt und welche Meldungen, in denen der Erkennungscode erkannt wird, an einen zweiten Ausgang führt. Dieser vorzugsweise softwaremässig auf der Chipkarte aufgebaute Filter wird stets angesprochen, wenn das Endgerät, insbesondere das Mobilfunkgerät, die Chipkarte mit dem Update "SMS Kommando" anspricht, d.h., wenn eine Meldung oder Kurznachricht auf der Chipkarte gespeichert werden soll. Meldungen, die aufgrund des korrekten Kennungscodes an den zweiten Ausgang geleitet werden, werden anschliessend auf korrekte Meldungs- bzw. Nachrichtensynchronisation überprüft. Falls diese nicht gegeben ist, wird die Meldung nicht akzeptiert. Falls die Meldungssynchronisation korrekt ist, wird die Meldung dahingehend überprüft, ob es sich um eine Teilnachricht oder um eine vollständige Einzelnachricht handelt.

Das Filter kann irgend eine Einrichtung sein, die geeignet ist, Datentelegramme, die den Kennungscode enthalten, zu erkennen und/oder auszuscheiden.

Erfindungsgemäss ist vorgeschlagen, dass im Kennungscode die Anzahl Teilnachrichten für eine vollständige Nachricht und eine Information für die Stellung der entsprechenden Teilnachricht innerhalb der Nachricht enthalten sind. Im Speichermittel der Chipkarte werden die einzelnen Meldungen in der Reihenfolge ihres Eintreffens mindestens so lange gespeichert, bis die vollständige Nachricht empfangen worden ist. Erst dann wird mit der Abarbeitung, und zwar in der richtigen Reihenfolge der einzelnen Meldungen, welche Reihenfolge nicht der Empfangsreihenfolge entsprechen muss, begonnen. Zentralenseitig ist vorgesehen, dass die zentrale Einheit für die besonderen Dienste eine Betriebszentrale umfassen, einen sogenannten SIM Service Center (SSC). Diesem SIM Service Center kann für jeden besonderen Dienst ein Logikmodul (SVL, Servicelogic) zugeordnet sein. Die einzelnen Logikmodule sind mit dem SIM Service Center funktionsmässig verbunden. Dem SIM Service Center ist im weiteren eine Datenbank zugeordnet, die unter anderem zum Verwalten von Berechtigungsdaten der Teilnehmer, die zum Übermitteln von Meldungen mit Kennungscode berechtigt sind, bestimmt ist. Eine Authentizitätskontrolleinheit (AUC, Authentication Center) ist ebenfalls funktionsmässig mit dem SIM Service Center verbun-

den. Dies ist ein Modul zum Berechnen, Verschlüsseln und Kontrollieren von einem im Kennungscode enthaltenen Sicherheitscode, dem Kryptogramm.

Auf die Art und Weise, wie der Sicherheitscode gebildet ist, wird weiter hinten eingegangen. Vorweggenommen sei lediglich, dass in diesen eine Zufallszahl mit einbezogen ist, wobei die Zufallszahl selbst, vorzugsweise eine durch den Betreiber des Kommunikationsnetzes definierbare Funktion der Meldung ist.

Im folgenden ist die Erfindung anhand von Figuren beispielsweise näher beschrieben. Es zeigen

Fig. 1 den prinzipiellen Aufbau eines nach dem GSM-Standard arbeitenden Mobilfunknetzes gemäss dem Stand der Technik,

Fig. 2 ein erfindungsgemäss erweitertes nach dem GSM-Standard arbeitendes Mobilfunknetz,

Fig. 3 ein Mobilfunktelefon mit einer Chipkarte für ein Mobilfunknetz gemäss den Fig. 1 und 2,

Fig. 4 ein erstes Flussdiagramm, das die Funktion des erfindungsgemässen Filters zeigt,

Fig. 5 ein zweites Flussdiagramm, aus dem die prinzipielle Arbeitsweise des Filters ersichtbar ist,

Fig. 6 den Aufbau eines Datentelegrammes einer Meldung SMS gemäss dem GSM-Standard,

Fig. 7 den Aufbau eines Datentelegrammes einer Meldung mit einem Kennungscode für besondere Dienste, und

Fig. 8 das Mobilfunknetz gemäss der Fig. 2, anders dargestellt, zum Erklären des Vorganges einer Nachrichtenübermittlung.

Ausgehend von einem vorzugsweise digital arbeitenden zellular aufgebauten Mobilfunknetz gemäss der Fig. 1, das nach dem GSM-Standard oder nach dem DCS 1800 Standard definiert ist, umfasst die erfindungsgemässe Vorrichtung zur Übermittlung von Meldungen, die in der Fig. 2 aufgeführten Netzerweiterungen.

Zum Senden und Empfangen von Meldungen, die in ihrem Datentelegramm den erfindungsgemässen Kennungscode enthalten, sind die dazu vorgesehenen Endgeräte 4, 9 mit einem Filter 12.1 ausgerüstet. Dieser Filter ist vorzugsweise ein Softwaremodul und entweder in einem Speicher im Endgerät selbst oder vorzugsweise auf einer Chipkarte enthalten, welche letztere in eine Schreib-Lese-Vorrichtung, welche am Endgerät 4 angeordnet ist, eingeführt werden kann.

Der Short Message Service Center (SMS-C) 8 leitet von Endgeräten 4,9 übermittelte Datentelegramme an eine Betriebszentrale für besondere Dienste (SSC, SIM Service Center) 10 weiter. Dieser Betriebszentrale ist ebenfalls ein Filter 12.2 zugeordnet, welches Datentelegramme ohne Kennungscode unmittelbar zum Short Message Service Center 8 zurückführt und lediglich solche mit ei-

nem Kennungscode weiterverarbeitet. Der Betriebszentrale ist vorzugsweise für jeden besonderen Dienst, wofür in der Beschreibungseinleitung ein Beispiel bereits kurz genannt ist, ein Logikmodul (SVL 1, SVL n, Service Logic) 11.1 bis 11.n zugeordnet. Mit 11.1 ist dabei das Logikmodul für einen ersten besonderen Dienst oder eine erste Anwendung und mit 11.n ein Logikmodul für einen n-ten besonderen Dienst oder eine n-te Anwendung bezeichnet. Die Anzahl der besonderen Dienste oder Anwendungen ist nicht beschränkt und im wesentlichen von der Kreativität des Netzbetreibers abhängig.

Der SIM Service Center 10 arbeitet zusammen mit Modulen 14, 15 zum Verwalten von Berechtigungsdaten einzelner Teilnehmer, die zum Übermitteln von Meldungen mit Kennungscode berechtigt sind, sowie zum Berechnen, Verschlüsseln und Kontrollieren von einem im Kennungscode enthaltenen Sicherheitscode. Das erste dieser Module ist im wesentlichen eine Datenbank 14, in welcher Teilnehmeridentifikationsdaten von Teilnehmern, die zum Benutzen der besonderen Dienste berechtigt sind, abgelegt sind. Im zweiten Modul 15 dem Authentication Center, wird insbesondere ein im Kennungscode enthaltener Sicherheitscode bei empfangenen Meldungen kontrolliert bzw. bei zu übermittelnden Meldungen berechnet und verschlüsselt. Ein Beispiel dazu ist weiter hinten aufgeführt.

Vorteilhafterweise ist dem SIM Service Center 10 ebenfalls eine Einheit für eine gesprochene Antwort VRU (Voice Respond Unit) 13 zugeordnet, die insbesondere einem Teilnehmer, der einen besonderen Dienst anfordert, mit gesprochenen Mitteilungen eine Unterstützung zum Zugreifen auf den gewünschten besonderen Dienst gewährt. In besonderen Fällen kann die VRU auch ein Help Desk sein, bei dem der gesprochene Text persönlich erfolgt.

Ein Mobilfunktelefon, wie es bei einer erfindungsgemässen Meldungsübermittlungsvorrichtung gemäss dem Ausführungsbeispiel üblicherweise verwendet wird, ist in der Fig. 3 dargestellt. Das Mobilfunktelefon umfasst dabei ein Bedienungsfeld bzw. eine Tastatur 16, ein Anzeigefeld, insbesondere in der Form einer LC-Anzeige 17, eine Antenne 18, eine Höreröffnung 19, hinter welcher ein Hörer zum Ausgeben einer Sprachkommunikation angeordnet ist, sowie eine Mikrophonöffnung 20, durch welche akustische Signale, die zu übermitteln sind, einem Mikrophon zugeführt wird. Am Mobilfunktelefon 4 ist ebenfalls eine Öffnung 21 zum Einführen einer Chipkarte vorgesehen. Innerhalb der Öffnung oder dem Schlitz 21 ist eine Schreib-Lese-Vorrichtung vorhanden, über welche ein Datenaustausch zwischen dem Endgerät und einer Chipkarte 22 erfolgen kann. Die Chipkarte 22 benötigt zum Ar-

beiten mit den besonderen Diensten mindestens einen Speicher von 8 Kilobytes EEPROM, welcher Speicher auf dem Chip 23 enthalten und in der Figur nicht näher dargestellt ist. Der Chip 23 ist über ein Kontaktfeld 24, welches aus mehreren einzelnen elektrischen Kontakten besteht, mit der im Mobilfunktelefon angeordneten Schreib-Lese-Vorrichtung elektrisch verbindbar. Auf dem Chip 23 ist mit dem Bezugszeichen 25 ein Speicherbereich gekennzeichnet, welcher ein Chipkartenbetriebssystem (COS Card Operating System) umfasst. Mit 26 ist derjenige Speicherbereich bezeichnet, in welchem das erfindungsgemässe Filter 12.1 abgelegt ist. Weitere Speicherbereiche, insbesondere zum temporären Speichern von mehreren Meldungen einer vollständigen Nachricht sind ebenfalls vorhanden, in den Figuren jedoch nicht speziell ersichtlich.

Wie das erfindungsgemässe Filter 12.1 zum Erkennen des Kennungscodes funktionsmässig ausgeführt und in das Betriebssystem auf dem Chip 23 einer Chipkarte eingefügt sein kann, geht aus den Fig. 4 und 5 hervor. Das Chipkartenbetriebssystem 25 ist dabei aufgeteilt in einen ersten Teil 25.1, welcher aus einem Informationsfluss, der zum Endgerät gelangt, insbesondere erkennt, ob darin ein Datentelegramm mit dem standardisierten Datenvorsatz oder Header vorhanden ist, der gemäss GSM 4.08 bzw. GSM 3.40 definiert ist. Falls eine solche Short Message erkannt wird, sorgt der erste Teil des Betriebssystems 25.1 dafür, dass das entsprechende Datentelegramm abgefangen wird. Mit dem erfindungsgemässen Filter 12.1 wird nun jedes erkannte Datentelegramm nach dem Vorhandensein des Kennungscodes 12.1 abgefragt. Wie bereits gesagt, stellt das Filter eine softwaremässige Verzweigungsschaltung mit einem Eingang und zwei Ausgängen dar, wobei Datentelegramme, die den Kennungscode nicht enthalten, direkt einem ersten Ausgang zugeführt werden, welcher mit dem Block 25.2, einem zweiten Teil des Betriebssystems verbunden ist. Ein solches Datentelegramm wird nun gemäss dem Stand der Technik auf der Chipkarte gespeichert. Dies geschieht üblicherweise anhand von Instruktionen, die beispielsweise im zweiten Teil 25.2 des Betriebssystems enthalten sein können. Falls das Filter einen Kennungscode erkennt, wird die entsprechende Meldung über einen zweiten Ausgang einem Modul 27 zum Abarbeiten eines besonderen Dienstes zugeführt. Im Kennungscode ist unter anderem eine Information enthalten, welche eine Aussage darüber macht, ob es sich bei der empfangenen Meldung um eine Einzelnachricht handelt, oder ob weitere Meldungen folgen, bis eine vollständige Nachricht übermittelt ist. In jedem Fall wird dem Endgerät mitgeteilt, die wievielte Meldung der Nachricht soeben empfangen worden ist. Dies ist

erforderlich, da die Meldungen innerhalb dem Kommunikationsnetz nach gewissen Prioritätskriterien übertragen werden, auf die hier nicht näher eingegangen werden soll, und die dafür verantwortlich sind, dass mehrere Meldungen einer Nachricht in irgend einer Reihenfolge beim Empfangsgerät eintreffen können, welche Reihenfolge nicht unbedingt der richtigen Reihenfolge entsprechen muss. Damit dadurch keine Schwierigkeiten entstehen, ist ein Speicherbereich oder Stack 28 auf dem Chip vorgesehen, auf welchem sämtliche Meldungen einer Nachricht abgespeichert werden, bis die gesamte Nachricht übermittelt worden ist. Erst danach wird mit der Abarbeitung der Nachricht begonnen. Bei einer Nachricht, die aus einer einzigen Meldung besteht, erfolgt selbstverständlich das Abarbeiten sofort.

In der Fig. 5 ist ein weiteres Flussdiagramm gezeigt, aus welchem die prinzipielle Arbeitsweise des erfindungsgemässen Filters ersichtlich ist. Sobald gemäss dem GSM Standard ein Datentelegramm als Meldung festgestellt worden ist (Block 29), wird in einem ersten Abfrageblock 30 geprüft, ob im Datentelegramm ein korrekter Kennungscode enthalten ist. Falls dies nicht zutrifft, wird die Meldung an den ersten Ausgang des Filters zum Block 25.2 weitergegeben. Bei Korrekterkennung, was durch erneutes Berechnen des einleitend bereits erwähnten Kryptogrammes und Vergleich mit dem übermittelten Kryptogramm durchgeführt wird, wird in einem zweiten Abfrageblock 31 im weiteren geprüft, ob die Synchronisation korrekt ist. Auf diese wie auf das Kryptogramm wird weiter hinten noch näher eingegangen. Bei unkorrekter Synchronisation wird das Datentelegramm direkt über den ersten Ausgang dem Block 25.2 übergeben. Bei korrekter Synchronisation wird in einem dritten Abfrageblock 32 festgestellt, ob die soeben empfangene Meldung eine vollständige Nachricht ist oder ob es sich lediglich um eine Teilnachricht handelt. Wie dies festgestellt wird, ist ebenfalls weiter hinten beschrieben. Handelt es sich bei der empfangenen Meldung um eine vollständige Nachricht, wird diese direkt dem Modul 27 zum unmittelbaren Abarbeiten zugeführt. Wird hingegen festgestellt, dass eine Meldung lediglich ein Teil einer Nachricht ist, so kann aus den vorgenannten Gründen eine Abarbeitung nicht erfolgen, solange nicht die ganze Nachricht vorhanden ist. In diesem Fall wird die Teilnachricht im dazu vorgesehenen Stack 28 mindestens so lange abgespeichert, bis alle Teilnachrichten vorhanden sind und mit der Abarbeitung begonnen werden kann. Dies wird im Entscheidungsblock 34 überwacht.

Das Filter 12.2, das vorzugsweise ebenfalls ein Softwaremodul ist und in einem der Betriebszentrale für besondere Dienste (SSC) vorhandenen Speicherbereich abgelegt ist, entspricht funktionsmäs-

sig dem soeben beschriebenen Filter.

Ein Datentelegramm zum Übermitteln einer Kurzmeldung mit dem standardisierten Short Message Service (SMS) ist in der Fig. 6 dargestellt. Das Datentelegramm 35 ist gemäss dem GSM Standard mit einer Länge von 176 Bytes definiert. Es umfasst einen Datenvorsatz oder Header 36, 37, welcher einen ersten Block 36 von 13 Bytes Länge umfasst, in welchem Teilnehmeradressdaten enthalten sind, die, wie bereits gesagt, gemäss dem GSM Standard 4.08 definiert sind. An den genannten ersten Block anschliessend ist im Header ein zweiter Block 37 vorhanden, welcher eine Länge von 23 Bytes aufweist und in welchem Short-Message-Service-spezifische Daten, die gemäss dem GSM Standard 3.40 definiert sind, enthalten sind. Auf die einzelnen Blöcke soll in diesem Zusammenhang nicht weiter eingegangen werden, da die entsprechenden Informationen den genannten Publikationen entnommen werden können.

Anschliessend an den Datenvorsatz sind in einem standardgemässen Datentelegramm 140 Bytes vorhanden, die im wesentlichen die Meldungsinformationen beinhalten.

In der Fig. 7 ist im Gegensatz zum soeben beschriebenen Datentelegramm ein Datentelegramm 39 dargestellt, das den erfindungsgemässen Kenncode 40, genannt Transport-Protocol-Data-Unit (TP-DU), umfasst. Das Datentelegramm ist gemäss dem GSM Standard ebenfalls 176 Bytes lang und schliesst den gleichen, aus den Blöcken 36, 37 bestehenden Datenvorsatz oder Header ein. Vorzugsweise anschliessend daran ist der Kennungscode 40 enthalten. Dieser ist wiederum aus mehreren Blöcken 41, 42, 43 aufgebaut. Diese für einen fehlerfreien Informationsfluss für Nachrichten, die besonderen Diensten zugeordnet sind, notwendigen Blöcke umfassen einen mit 41 gekennzeichneten ersten Block mit Angaben über die Anzahl Meldungen für eine vollständige Nachricht, Angaben über die Stellung der entsprechenden Meldung in der vollständigen Nachricht, sowie Angaben der ab einem Zeitpunkt t_0 total übermittelten Anzahl Meldungen. Der Block 42 umfasst Daten über die Synchronisation der Nachrichten, auf welche weiter hinten noch näher eingegangen wird. Das gleiche gilt für den Block 43, in welchem aus den Daten des Blockes 42 sowie aus geheimen Daten, die sowohl auf der Sendeseite wie auf der Empfangsseite gespeichert sind, ein errechneter Sicherheitscode abgelegt ist. Beim Mobilfunkgerät sind die geheimen Daten auf der Chipkarte enthalten und beim SIM Service Center in der diesem zugeordneten Datenbank. Weitere Informationen dazu sind ebenfalls nachfolgend anhand der Erklärung des Vorganges einer Nachrichtenübermittlung beschrieben.

Ein solcher Vorgang einer Nachrichtenübermittlung ist aus der Fig. 8 ersichtlich. Dort ist das Mobilfunknetz gemäss der Fig. 2 in einer Darstellung gezeichnet, die sich zum Erklären des oben genannten Vorganges besser eignet. In der gewählten Darstellung sind die Funkzellen 2, die Basisstationen 3 die Controller für mehrere Basisstationen 5, die Mobilfunkzentrale 6 sowie ein damit in Verbindung stehendes drahtgebundenes Telefonnetz 7 in einem einzigen Feld zusammengefasst. Ausserhalb dieses Feldes sind zwei Endgeräte, insbesondere Mobilfunktelefone 4 mit je einer Chipkarte 22 gezeichnet. Die beiden Mobilfunktelefone 4 seien einem Teilnehmer A und einem Teilnehmer B zugeordnet. Ebenfalls ausserhalb des gemeinsamen Feldes ist die Zentrale für den Kurzmeldungsdienst SMS-C, (Short Message Service-Center) 8 gezeichnet. Funktionsmässig an das Short Message Service Center 8 angeschlossen ist erfindungsgemäss die Betriebszentrale für die besonderen Dienste (SSC, SIM Service Center) 10 mit dem Filter 12.2. Der Betriebszentrale zugeordnet sind, wie bereits gesagt, die Service Logic Module 11.1 bis 11.n je eines für einen besonderen Dienst. In der Fig. 8 ebenfalls ausserhalb des gemeinsamen Feldes sichtbar sind die beiden Module 14 und 15 bzw. das Datenbankmodul 14 und die Authentizitätskontrolleinheit 15. Im weiteren ist die Einheit für eine gesprochene Antwort oder Voice Respond Unit (VRU) 13 sichtbar.

Der Teilnehmer A, der seine persönliche Chipkarte 22 in ein Mobilfunkgerät 4 eingeführt hat und durch diese Chipkarte gekennzeichnet und identifiziert ist, ruft mit den Tasten auf seinem Bedienungsfeld eine Servicenummer an. Dies kann beispielsweise eine gebührenfreie Telefonnummer sein. Dieser Anruf gelangt über die nicht dargestellte Mobilfunkzentrale zur Voice Respond Unit 13. Diese fordert den Teilnehmer A mittels einer Sprachansage auf, einen Dienst auszuwählen.

Nach erfolgter Dienstausswahl, welche wiederum mit den Tasten des Bedienungsfeldes vom Teilnehmer A erfolgt, signalisiert die Voice Respond Unit 13 dem SIM Service Center 10, dass der Teilnehmer A beispielsweise den Dienst SVL 1 ausgewählt hat. Dabei kann die Voice Respond Unit 13 entweder die Rufnummer des rufenden Teilnehmers automatisch ermitteln (Calling Number Identification) oder diese wiederum über eine Sprachausgabe beim rufenden Teilnehmer erfragen. Dieser Informationsfluss ist in der Figur mit a, b bezeichnet.

Das SIM Service Center 10 prüft nun anhand der Datenbank 14, ob der Kunde bekannt und für den Dienst SVL 1 berechtigt ist. Wenn nein, wird beispielsweise die Anfrage durch eine entsprechende Ansage der Voice Respond Unit zurückgewiesen. Wenn ja, wird die erste Nachricht für den

gewünschten Dienst SVL1 gebildet, und mittels Aufruf des Authentication Centers 14 ein Sicherheitscode, das Kryptogramm gebildet. Die Bildung eines solchen Kryptogrammes oder eines nach bestimmten Regeln verschlüsselten Wortes kann beispielsweise nach dem bekannten DES-Standard erfolgen.

Dieser gehorcht beispielsweise einer Gleichung

$$SRES = A3(ki, RAND).$$

Darin bedeuten:

SRES Signed Responds / Nachrichtenantwort,

A3 geheimer Algorithmus, der sowohl im Authentication Center 15 als auch auf der Chipkarte 22 gespeichert ist,

ki geheimer Schlüssel, der ebenfalls sowohl im Authentication Center 15 als auch auf der Karte 22 des entsprechenden Teilnehmers vorhanden ist,

RAND Random / Zufallszahl oder Prüfsumme, die beispielsweise aus dem Inhalt der ersten Nachricht erfindungsgemäss wie folgt gewonnen wird:

$$RAND = f(\text{Nachricht}).$$

Die Funktion, nach welcher die Zufallszahl oder Prüfsumme aus der Nachricht gewonnen werden soll, kann beispielsweise vom Teilnehmer selbst anlässlich einer Identifikationsprozedur beim erstmaligen Einsatz der Chipkarte, auf welche Prozedur aber hier nicht näher eingegangen werden soll, festgelegt werden. Es kann irgend eine mathematische Funktion sein, die irgendwie beispielsweise mit der Länge der Nachricht verknüpft wird. Die Zufallszahl oder Prüfsumme RAND, oder die Funktion nach welcher diese Zahl berechnet werden soll, sind auf der Chipkarte 22 und im Authentication Center 15 gespeichert und werden jeweils an Ort berechnet.

Das gemäss den genannten Formeln berechnete Kryptogramm SRES wird im Block 43 des Kennungscodes 40 im Datentelegramm für die erste Meldung abgelegt. Über die Datenbank 14 wird der aktuelle Synchronisationszähler für die Chipkarte 22 des Teilnehmers A festgestellt. Der Inhalt des Synchronisationszählers ist ebenfalls Teil des Kennungscodes und wird im Block 42 abgelegt. In den Block 41 des Kennungscodes wird eingeschrieben wieviele Meldungen die angeforderte und an den Teilnehmer A zu übermittelnde Nachricht umfasst und welche Meldung innerhalb einer Meldungsfolge soeben aufbereitet wird. Diese Vorgänge sind in der Fig. 8 mit dem Buchstaben c bezeichnet.

Das SIM Service Center 10 schickt nun die auf diese Weise aufbereitete Nachricht, die aus einer oder mehreren Meldungen bzw. Datentelegrammen bestehen kann, an den Teilnehmer A bzw. an des-

sen Chipkarte 22, die in einem Endgerät 4 eingesteckt ist. Alle Nachrichten werden dabei, wie eingangs genannt, als GSM Klasse 2 Nachrichten verschickt. Das Verschicken einer solchen Nachricht ist mit dem Buchstaben d gekennzeichnet. Sobald eine Nachricht, die die Prüfkriterien des Filters auf der Chipkarte durchlaufen hat, auf der Chipkarte des Teilnehmers A gespeichert ist, wird durch diese eine positive Rückantwort, die mit e bezeichnet ist, generiert und dem SIM Service Center zurückgesandt.

Gemäss dem GSM Standard werden alle Nachrichten über ein Short Message Center (SMS-C) 8 sowohl gesendet als auch empfangen.

Der erfindungsgemässe Filter 12.1, der in einem Speicherbereich auf der Chipkarte 22 des Teilnehmers A enthalten ist, erkennt die eingehenden Nachrichten, sammelt Teilnachrichten im Chipkartenstack 28 und führt die Kartenanwendung dann aus, wenn alle Teilnachrichten eingetroffen sind. Dies kann anhand des Blockes 41 aus dem Kennungscodes 40 ermittelt werden.

Die Karte kann z.B. als Resultat der empfangenen Nachrichten neue, abgehende Nachrichten generieren und diese als Kurzmeldungen SMS MO-PP, (siehe unterster Abschnitt, Seite 2) an das Short Message Service Center 8 senden, welches die Nachrichten aufgrund des Kennungscodes an das SIM Service Center 10 weiterleitet. Eine solche Nachricht ist mit dem Buchstaben f in der Fig. 8 gekennzeichnet.

Ein Zyklus d, e, f kann sich je nach dem gewünschten besonderen Dienst und je nach dem angewählten Logikmodul 11.1 bis 11.n beliebige Male wiederholen. Das SIM Service Center 10 erhöht dabei mit jeder Nachricht den Synchronisationszähler pro Karte und bildet je Nachricht ein entsprechendes Kryptogramm, so dass die Chipkarte des Teilnehmers A die Authentizität der Daten prüfen kann. Die Rückantworten von der Chipkarte des Teilnehmers A an das SIM Service Center 10 sind vorzugsweise ebenfalls gemäss den vorstehenden Formeln verschlüsselt.

Die Reihenfolge der Blöcke 41, 42, 43 ist für die Erfindung nicht wesentlich und kann beliebig sein.

Patentansprüche

1. Vorrichtung zur Übermittlung von Meldungen in einem Kommunikationsnetz zur Sprach- und Datenverarbeitung mit einer Vielzahl von Endgeräten (4, 9), welche einem bestimmten Benutzer zugeordnet sind, oder mittels einem in das Endgerät einsetzbaren Datenträger (22) einem bestimmten Benutzer zugeordnet werden können, wobei mindestens zwei Endgeräte (4, 9) miteinander in eine Sprach- oder Datenkom-

munikation treten können, sowie mit mindestens einer Zentrale (8) zum Steuern der Meldungsübermittlung innerhalb dem Kommunikationsnetz, wobei jede Meldungsübermittlung eine Datenkommunikation ist bei welcher Datentelegramme (35, 39) ausgetauscht werden, in welchen ein standardisierter Datenvorsatz (36, 37) enthalten ist, dadurch gekennzeichnet, dass Datentelegramme (39) zusätzlich zum standardisierten Datenvorsatz (36, 37) einen Kennungscodes (40) enthalten können, dass mindestens eine im Kommunikationsnetz vorhandene zentrale Einheit (10) und mindestens ein Teil der Endgeräte (4, 9) Mittel zum Erzeugen von mit dem Kennungscodes (40) versehenen Datentelegrammen (39) aufweisen, wobei die Datentelegramme entweder von der zentralen Einheit (10) zu mindestens einem der Endgeräte (4, 9) oder von einem der Endgeräte zur zentralen Einheit übermittelt werden, dass Filter (12.1, 12.2) zum Erkennen des Kennungscodes vorhanden sind, wobei der zentralen Einheit sowie mindestens dem genannten Teil der Endgeräte je eines der Filter zugeordnet ist, und wobei der Kennungscodes dazu vorgesehen ist, der zentralen Einheit oder dem Endgerät mitzuteilen, dass die in der Meldung enthaltenen Daten (4, 5) nach einer speziellen, sonst nicht zugänglichen Prozedur zu verarbeiten sind.

2. Vorrichtung nach Anspruch 1, dadurch gekennzeichnet dass das Kommunikationsnetz ein digital arbeitendes Kommunikationsnetz, insbesondere ein zellular aufgebautes Mobilfunknetz (1) nach dem GSM-oder dem DCS1800-Standard ist.
3. Vorrichtung nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die den Endgeräten (4, 9) zugeordneten Filter (12.1, 12.2) je ein Softwaremodule ist, das in einem Speichermittel (26), welches im Endgerät (4, 9) oder auf dem Datenträger (22) vorhanden ist, enthalten ist.
4. Vorrichtung nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass mindestens ein Teil der Endgeräte Mobilfunktelefone (4) sind, die je eine Vorrichtung (21) zum Austauschen von Daten mit dem Datenträger, insbesondere mit einer in das Mobilfunktelefon einsetzbaren Chipkarte (22) umfassen.
5. System nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass Datentelegramme (39), die den Kennungscodes (40) enthalten, lediglich ein Teil einer Nachricht, bestehend aus mehreren Datentelegrammen (39) sind,

wobei in jedem Datentelegramm im Kennungscode die Anzahl Datentelegramme für die vollständige Nachricht und eine Information für die Stellung eines entsprechenden Datentelegrammes innerhalb der Nachricht enthalten sind.

5

6. Vorrichtung nach Anspruch 5, dadurch gekennzeichnet, dass ein Kontrollmittel (32) vorhanden ist, das derart wirkt, dass jedes zu einer Nachricht gehörende Datentelegramm im Speicher-
mittel (25, 26) gespeichert wird und dass die weitere Verarbeitung der Datentelegramme erst dann erfolgt wenn die vollständige Nachricht im Speicher-
mittel vorhanden ist.

10

15

7. Vorrichtung nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass der Kennungscode (40) dem standardisierten Datenvorsatz (36, 37) nachgeordnet ist.

20

8. Vorrichtung nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass der zentralen Einheit (10) Module (14, 15) zum Verwalten von Berechtigungsdaten einzelner Teilnehmer, die zum Übermitteln von Meldungen (39) mit Kennungscode (40) berechtigt sind und zum Berechnen, Verschlüsseln und Kontrollieren von einem im Kennungscode (40) enthaltenen Sicherheitscode zugeordnet sind.

25

30

9. Vorrichtung nach Anspruch 8, dadurch gekennzeichnet, dass in den Sicherheitscode (43) der Wert einer Zufallszahl (RAND) miteinbezogen ist, wobei die Zufallszahl selbst vorzugsweise eine durch den Betreiber des Kommunikationsnetzes definierbare Funktion der Meldung ist.

35

10. Vorrichtung nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, dass die mit dem Kennungscode (40) versehenen Meldungen (39) Bestandteile von besonderen Diensten, die vom Kommunikationsnetzbetreiber angeboten werden, sind.

40

45

50

55

Fig. 1

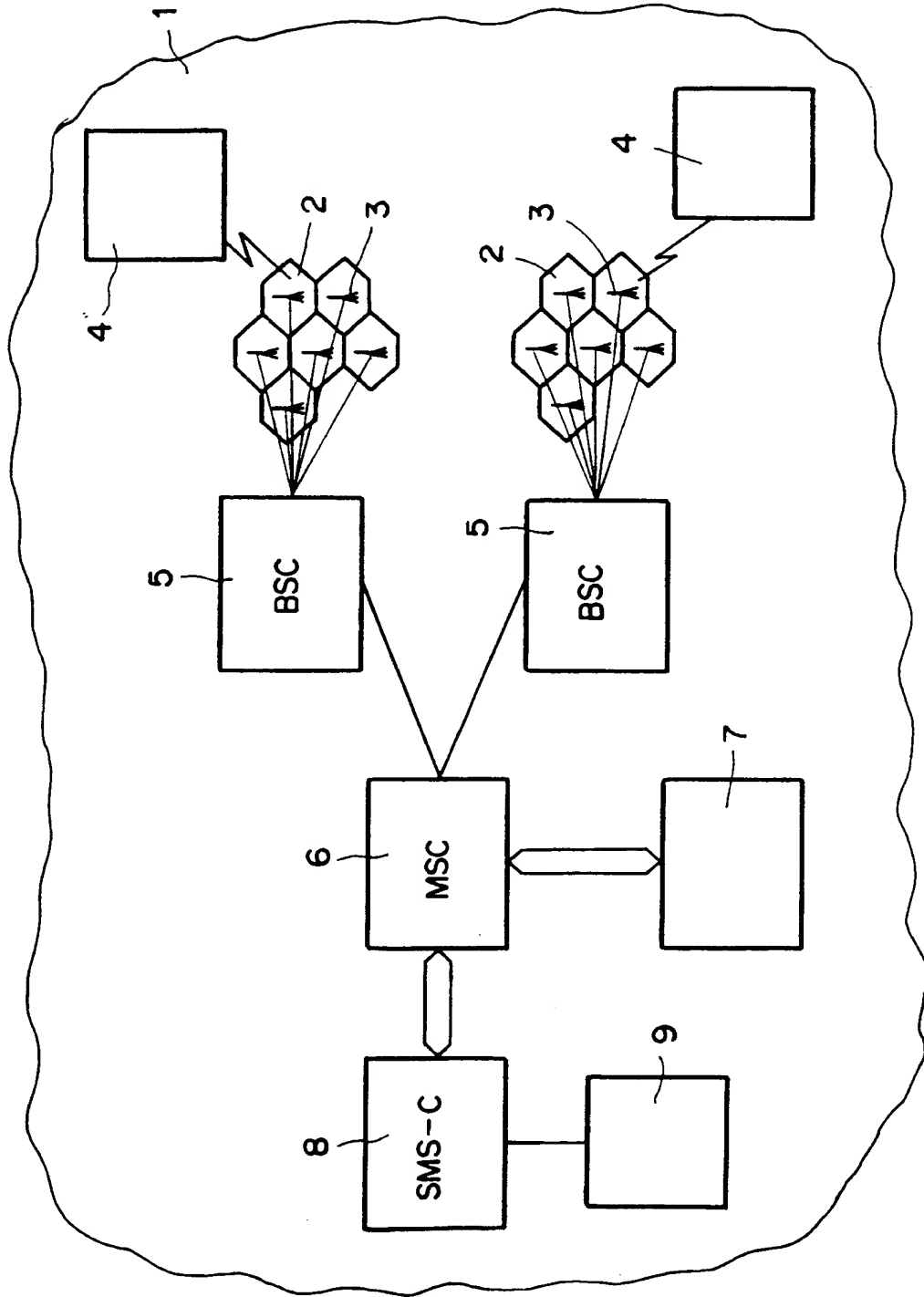


Fig. 2

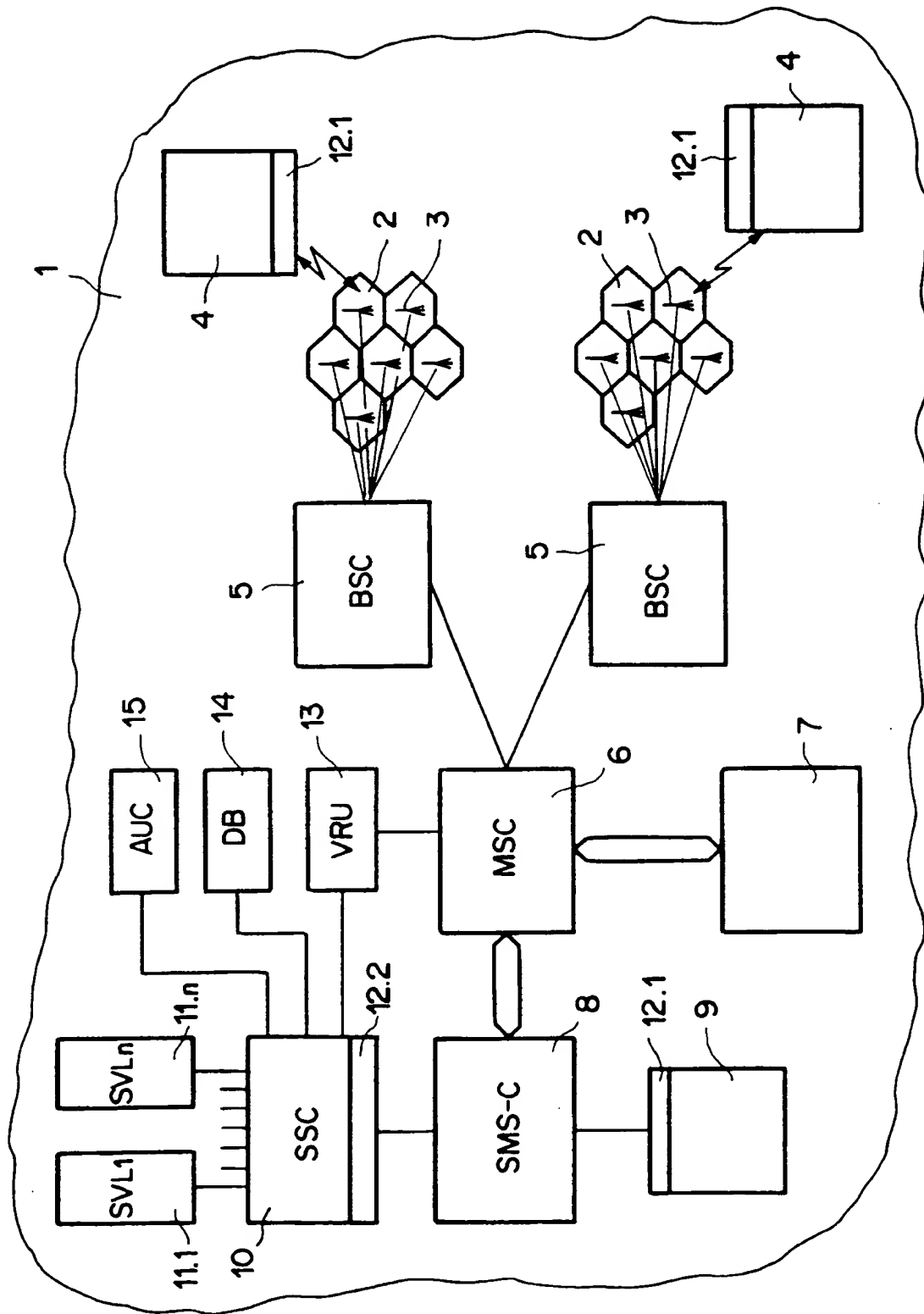
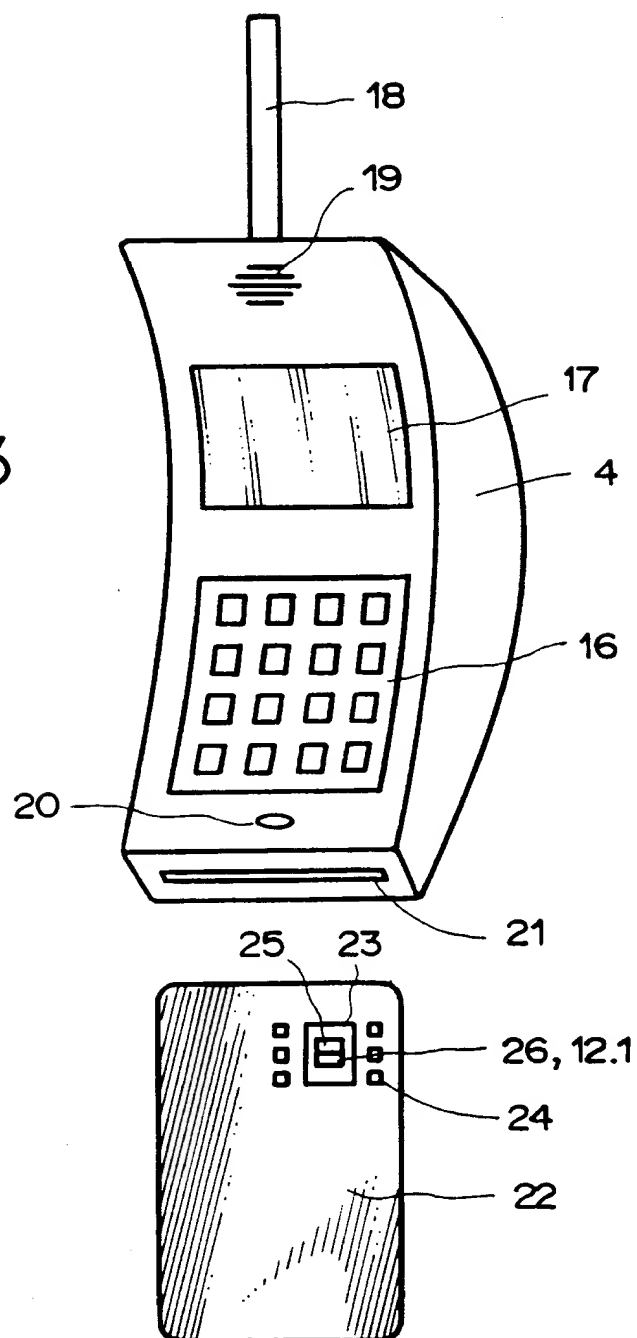


Fig. 3



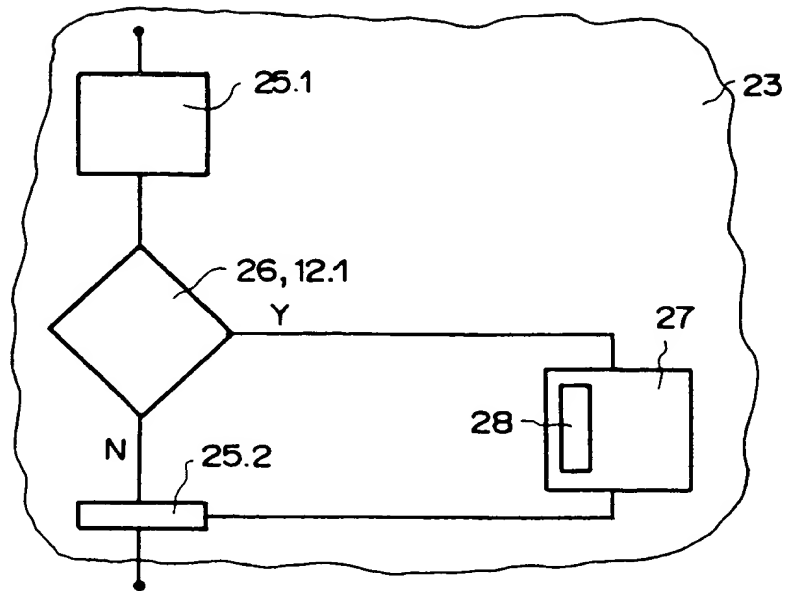


Fig. 4

Fig. 6

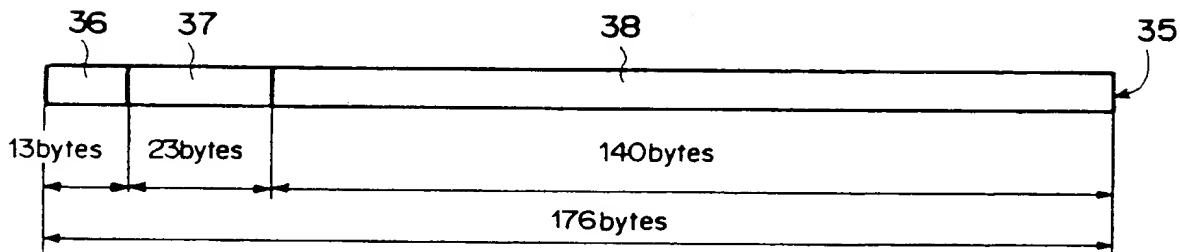


Fig. 7

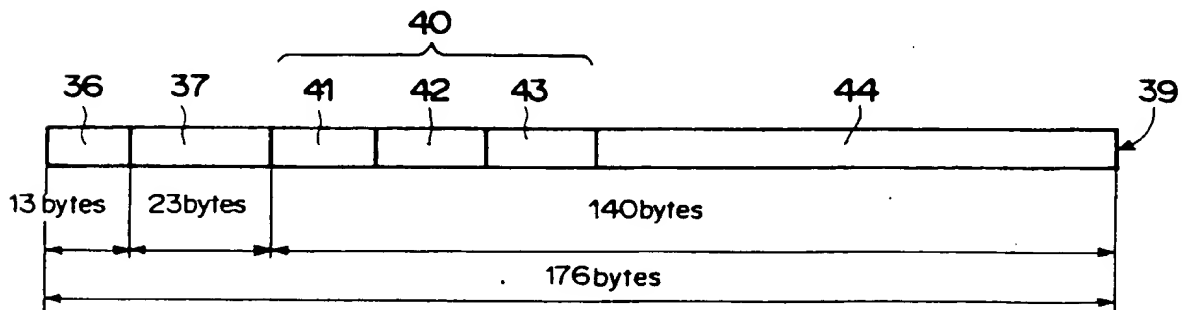


Fig. 5

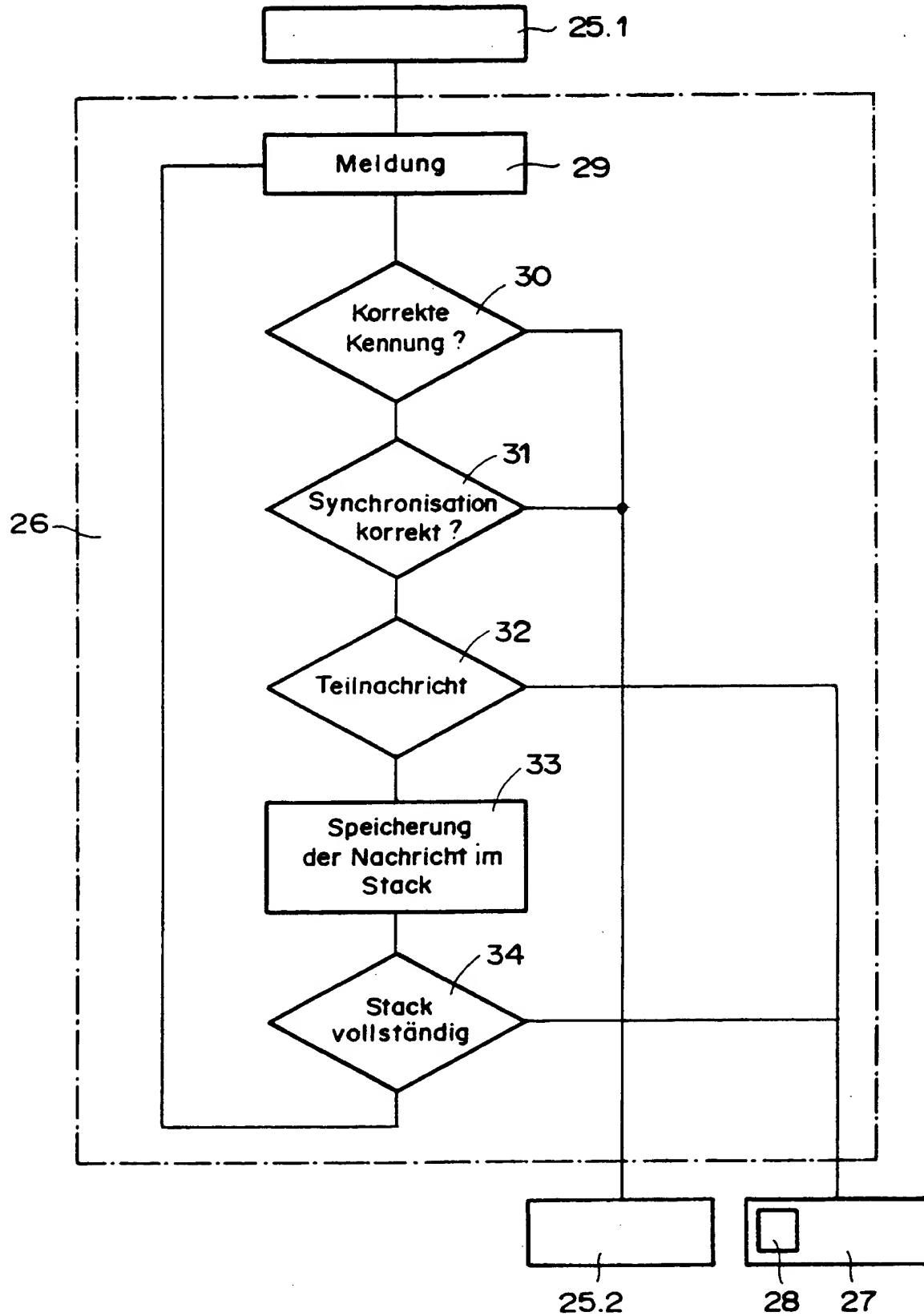
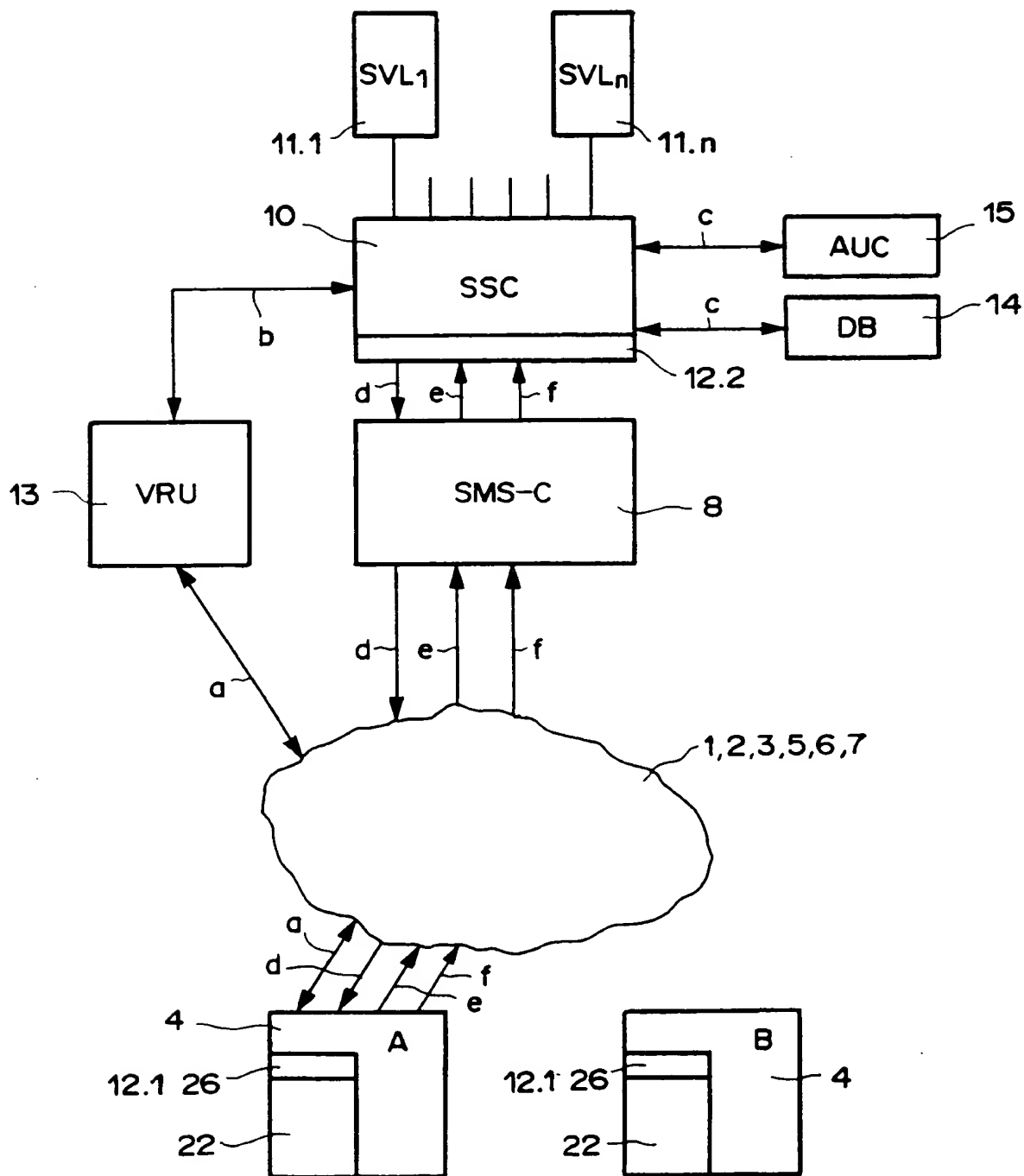


Fig. 8





Europäisches
Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 94 81 0363

EINSCHLÄGIGE DOKUMENTE			
Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Retrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int.Cl.6)
X	EP-A-0 555 992 (NOKIA)	1-4,7-10	H04Q7/22
Y	* Spalte 2, Zeile 56 - Spalte 4, Zeile 28; Abbildung *	5,6	

X	EP-A-0 562 890 (HUTCHISON MICROTREL)	1-4,7-10	
Y	* Spalte 3, Zeile 1 - Zeile 21 *		
Y	* Spalte 3, Zeile 51 - Spalte 6, Zeile 53; Abbildungen *	5,6	

X	WO-A-92 14329 (TELENOKIA)	1-4,8-10	
	* Seite 2, Zeile 13 - Seite 3, Zeile 2 *		
	* Seite 7, Zeile 20 - Seite 11, Zeile 10 *		
	* Seite 12, Zeile 32 - Seite 13, Zeile 10 *		
Y	* Seite 14, Zeile 24 - Seite 16, Zeile 34 *	5,6	

Y	CH-A-683 052 (ERIKA KÖCHLER)	5,6	
	* Seite 2, Zeile 41 - Zeile 57 *		
	* Seite 4, Zeile 3 - Seite 5, Zeile 41 *		

A	TELECOMMUNICATION JOURNAL OF AUSTRALIA, Bd.43, Nr.2, 1993, AU Seiten 33 - 38 GRIGOROVA ET AL. 'sim cards' * Seite 33-34, Absatz: SIM FUNCTIONALITY * * Seite 35-37, Absatz: AUTHENTICATION AND CIPHERING PROCESS *	1,8-10	RECHERCHIERTE SACHGEBIETE (Int.Cl.6) H04Q

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt			
Recherchenort		Abschließdatum der Recherche	
DEN HAAG		22. November 1994	
		Prüfer	
		Janyszek, J-M	
KATEGORIE DER GENANNTEN DOKUMENTE			
X : von besonderer Bedeutung allein betrachtet		T : der Erfindung zugrunde liegende Theorien oder Grundsätze	
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie		E : älteres Patentedokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist	
A : technologischer Hintergrund		D : in der Anmeldung angeführtes Dokument	
O : mchtschriftliche Offenbarung		L : aus andern Gründen angeführtes Dokument	
P : Zwischenliteratur		& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument	



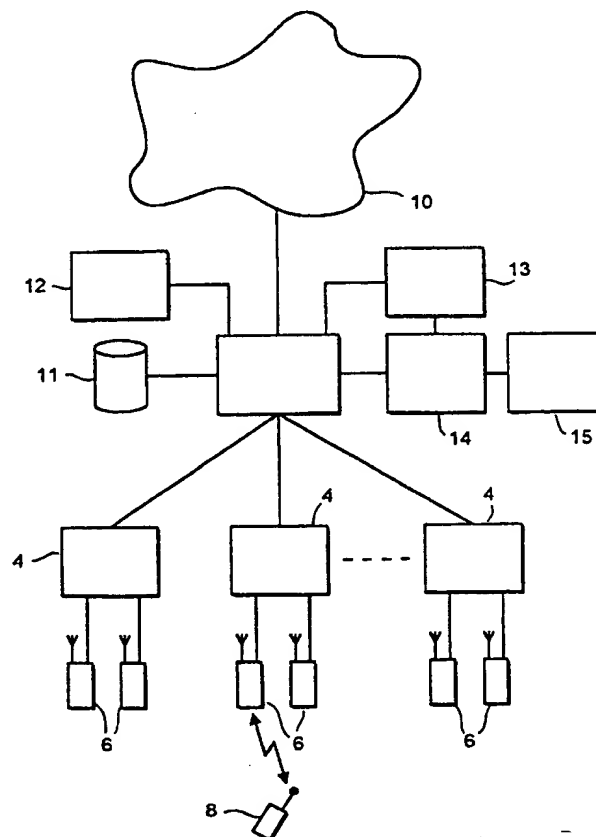
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : H04Q 7/22, 7/32		A1	(11) International Publication Number: WO 99/04583
			(43) International Publication Date: 28 January 1999 (28.01.99)
(21) International Application Number: PCT/GB98/02064 (22) International Filing Date: 13 July 1998 (13.07.98) (30) Priority Data: 9715097.3 17 July 1997 (17.07.97) GB (71) Applicant (for all designated States except US): ORANGE PERSONAL COMMUNICATIONS SERVICES LIMITED [GB/GB]; St. James Court, Great Park Road, Almondsbury, Bristol BS12 4QJ (GB). (72) Inventor; and (75) Inventor/Applicant (for US only): FORD, Peter [GB/GB]; 18 Summers Mead, Yate, Bristol BS17 5RB (GB). (74) Agents: MUSKER, David, C. et al.; R.G.C. Jenkins & Co., 26 Caxton Street, London SW1H 0RJ (GB).		(81) Designated States: AL, AM, AT, AT (Utility model), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG). Published <i>With international search report.</i> <i>Before the expiration of the time limit for amending the</i> <i>claims and to be republished in the event of the receipt of</i> <i>amendments.</i>	

(54) Title: ENCRYPTED BROADCAST MESSAGES IN A CELLULAR COMMUNICATIONS SYSTEM

(57) Abstract

A method is described which provides functionality allowing mobile stations (8) of users having certain access rights to display messages broadcast on a common channel of a cell in a cellular telecommunications network in intelligible form. The messages, before broadcast, are encrypted using a predefined encryption key, and the mobile stations (8) having a corresponding access right are provisioned with the corresponding decryption key. Mobile stations lacking the appropriate access right are able to display a message, when received and picked up, only in encrypted, i.e. unintelligible, form. Some types of message broadcast within the cell on the same common channel are deemed general access messages, which are broadcast in unencrypted form and may be displayed in intelligible form by any mobile station (8) camped on to the cell in which the message is broadcast.



THIS PAGE BLANK (USPTO)

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav	TM	Turkmenistan
BF	Burkina Faso	GR	Greece		Republic of Macedonia	TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's	NZ	New Zealand		
CM	Cameroon		Republic of Korea	PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakhstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

International Application No

PCT/GB 98/02064

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04Q7/22 H04Q7/32

According to International Patent Classification(IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 96 41493 A (ERICSSON TELEFON AB L M) 19 December 1996	1,2,6, 13-16, 18-21,25
Y	see page 40, line 5 - page 41, line 2 see page 52, line 20 - page 53, line 17 see page 55, line 10 - line 17 see page 57, line 19 - page 58, line 6 see claims 1-10 --- -/--	3,7,8, 12,17,22

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search

10 November 1998

Date of mailing of the international search report

18/11/1998

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Baas, G

THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

International Application No

PCT/GB 98/02064

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	FARRUGIA A J ET AL: "SMART CARD TECHNOLOGY APPLIED TO THE FUTURE EUROPEAN CELLULAR TELEPHONE ON THE DIGITAL D-NETWORK" SELECTED PAPERS FROM THE SECOND INTERNATIONAL SMART CARD 2000 CONFERENCE, 4-6 OCTOBER 1989, AMSTERDAM, NL, 1 January 1989, pages 95-107, XP000472724 see page 100, line 1 - page 103, line 21 ---	3,7,8, 12,22
Y	US 5 371 493 A (SHARPE ANTHONY K ET AL) 6 December 1994 see column 3, line 3 - line 10 see column 6, line 35 - line 42 ---	17
A	EP 0 689 368 A (PTT GENERALDIREKTION) 27 December 1995 -----	

THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

information on patent family members

International Application No

PCT/GB 98/02064

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9641493 A	19-12-1996	US 5768276 A AU 6020296 A	16-06-1998 30-12-1996
US 5371493 A	06-12-1994	DE 69219991 D DE 69219991 T EP 0538933 A JP 5218946 A SG 48347 A	03-07-1997 27-11-1997 28-04-1993 27-08-1993 17-04-1998
EP 0689368 A	27-12-1995	AT 153206 T AU 691271 B AU 2174595 A BR 9508091 A CA 2152215 A WO 9535635 A CN 1128476 A CZ 9603513 A DE 59402759 D DK 689368 T ES 2103557 T FI 965078 A GR 3023908 T HU 76397 A JP 8265843 A NO 965315 A NZ 287390 A PL 317643 A SG 34235 A SI 9520064 A SK 161396 A ZA 9505091 A	15-05-1997 14-05-1998 04-01-1996 12-08-1997 21-12-1995 28-12-1995 07-08-1996 14-05-1997 19-06-1997 08-12-1997 16-09-1997 17-12-1996 30-09-1997 28-08-1997 11-10-1996 18-02-1997 19-12-1997 14-04-1997 06-12-1996 30-04-1997 05-11-1997 10-04-1996

THIS PAGE BLANK (USP10)

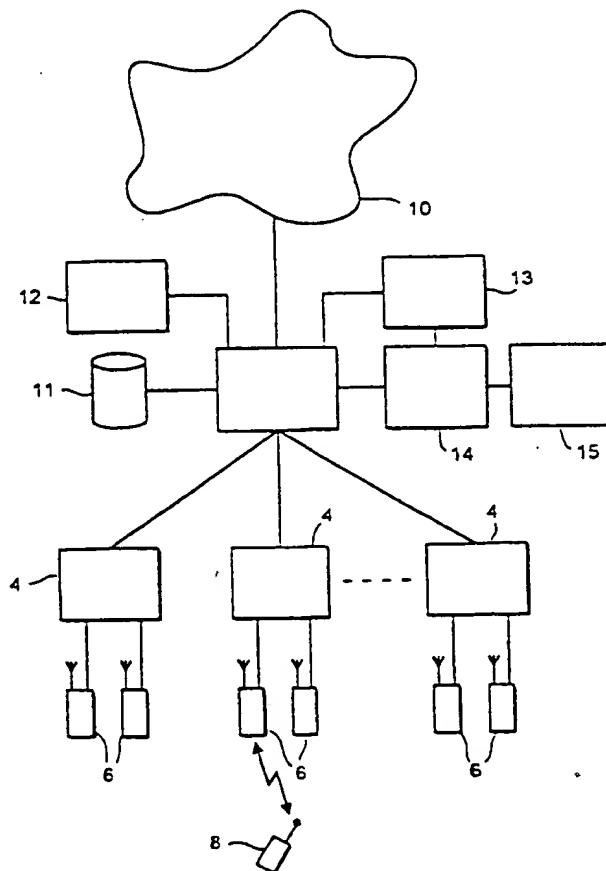
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : H04Q 7/22, 7/32	A1	(11) International Publication Number: WO 99/04583 (43) International Publication Date: 28 January 1999 (28.01.99)
<p>(21) International Application Number: PCT/GB98/02064</p> <p>(22) International Filing Date: 13 July 1998 (13.07.98)</p> <p>(30) Priority Data: 9715097.3 17 July 1997 (17.07.97) GB</p> <p>(71) Applicant (for all designated States except US): ORANGE PERSONAL COMMUNICATIONS SERVICES LIMITED [GB/GB]; St. James Court, Great Park Road, Almondsbury, Bristol BS12 4QJ (GB).</p> <p>(72) Inventor; and (75) Inventor/Applicant (for US only): FORD, Peter [GB/GB]; 18 Summers Mead, Yate, Bristol BS17 5RB (GB).</p> <p>(74) Agents: MUSKER, David, C. et al.; R.G.C. Jenkins & Co., 26 Caxton Street, London SW1H 0RJ (GB).</p>	<p>(81) Designated States: AL, AM, AT, AT (Utility model), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).</p> <p>Published With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</p>	

(54) Title: ENCRYPTED BROADCAST MESSAGES IN A CELLULAR COMMUNICATIONS SYSTEM

(57) Abstract

A method is described which provides functionality allowing mobile stations (8) of users having certain access rights to display messages broadcast on a common channel of a cell in a cellular telecommunications network in intelligible form. The messages, before broadcast, are encrypted using a predefined encryption key, and the mobile stations (8) having a corresponding access right are provisioned with the corresponding decryption key. Mobile stations lacking the appropriate access right are able to display a message, when received and picked up, only in encrypted, i.e. unintelligible, form. Some types of message broadcast within the cell on the same common channel are deemed general access messages, which are broadcast in unencrypted form and may be displayed in intelligible form by any mobile station (8) camped on to the cell in which the message is broadcast.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Larvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

09 / 4 6 3 1 4 6

420 Rec'd PCT/PTO 1 8 JAN 2000

ENCRYPTED BROADCAST MESSAGES IN A CELLULAR COMMUNICATIONS SYSTEM

This invention relates to a method of an apparatus for distributing and receiving information in a cellular telecommunications network, for example a GSM (Global System for Mobile communications) digital cellular radio network.

The GSM standard is defined in a set of technical specifications issued by the European Telecommunications Standards Institute (ETSI), and there are currently a number of mobile telecommunications networks operating in accordance with the GSM standard, and variants thereof, such as the DCS1800 standard.

One service provided is a service referred to as a cell broadcast (CB), or short message - cell broadcast (SMS CB), service. In this service, information in the form of pages of text is transmitted on a common channel (the cell broadcast channel, CBCH) of cells in the network. The transmission of pages is repeated at regular intervals, and users can store the information for retrieval and display by means of selective keystrokes on a mobile station, or may turn off the cell broadcast function so as not to store the information. The information is intended to include locality-specific information, such as lists of local facilities (hospitals, pharmacies, taxis, etc), local weather reports, local date/time indications, etc.

At present, however, the cell broadcast functionality, although provided for in current GSM-type networks and the mobile stations used in them, has not been widely implemented in practice, in probability at least partly due to the costs associated with assembling and disseminating information via the service.

5 In accordance with an aspect of the present invention there is provided a method of distributing information to users in a cellular telecommunications network comprising a mobile switching centre and a plurality of base stations transceiving in a plurality of cells of said network, said method comprising:

providing a plurality of mobile stations, each of said mobile stations
10 having an associated information access status;

broadcasting a signal on a common channel of at least one cell of said network, said signal containing a limited access message in encrypted form, for general reception in said at least one cell;

enabling first mobile stations having a first information access status to
15 decrypt and present said message to a user in unencrypted form when being served by said cell; and

preventing second mobile stations having a second information access status from presenting said message in unencrypted form to a user when being served in said cell.

20 An advantage of this aspect of the invention is that a user not authorised to access the information can only view the message in encrypted form and unintelligibly, whereas a user having access rights to the information is able to

view the message in decrypted and intelligible form services may be provided on a subscription basis. Some subscribers in the network may wish to have access to the information broadcast generally in the cell in addition to other services provided in the telecommunications network, such as voice call services, and will take out a subscription allowing access to the cellular information broadcasting service. Other users may not wish to receive the benefit of the information broadcast in the cell, and will take out a subscription, perhaps at lower cost, preventing them from accessing the information.

Preferably, the signal comprises a plurality of limited access messages each having a corresponding access right, the method comprising providing mobile stations with access rights, and enabling only mobile stations having an access right corresponding to a limited access message to present the limited access message to a user when being served in the cell. This allows the selection on a per user basis of the type of information a user is able to access, thus allowing a subscription to be individually tailored to a subscribers' needs.

The signal may also contain a general access message, the method comprising enabling both the first and second mobile stations to present the general access message to a user when being served in the cell. This allows both limited access messages and general access messages to be disseminated by broadcasts in cells of a cellular telecommunications system, allowing some information to be presented to any user irrespective of the subscription type held.

Preferably, alternative limited access messages are broadcast in cells located in different areas of the cellular telecommunications network, thereby tailoring the information within the messages to different localities and increasing the utility of the service.

5 In accordance with a further aspect of the invention there is provided apparatus for receiving information in a cellular telecommunications system, said apparatus comprising:

means for storing a decryption key;

10 means for receiving a message on a common channel in a cell of said cellular telecommunications system; and

means for decrypting said message using said stored decryption key; and

means for displaying said decrypted message to a user.

This aspect provides apparatus whereby a user may receive limited access messages on a common channel of a cell in the telecommunications system, and view the information in decrypted form, if the mobile station of the user is provided with the decryption key. A decryption key may be distributed only to cellular users having a predetermined subscription type.

15

An embodiment of the present invention will now be described, by way of example only, with reference to the accompanying drawings, wherein:

20 Figure 1 is a block diagram schematically illustrating a cellular telecommunicationssystem;

Figure 2 is a block diagram schematically illustrating a cellular telecommunications mobile station;

Figure 3 illustrates a list stored in a cell broadcast centre in accordance with the present invention;

5 Figure 4 is a flow diagram illustrating functions carried out by the cell broadcast centre in accordance with the present invention;

Figures 5 and 6 illustrate data blocks broadcast in a cell in accordance with the present invention;

10 Figure 7 is a flow diagram illustrating functions carried out by a network management centre in accordance with the present invention;

Figure 8 illustrates a short message transmitted to a mobile station in accordance with the present invention;

Figure 9 illustrates functions carried out by a mobile station when displaying a cell broadcast message in accordance with the present invention;

15 Figure 10 shows an example of a display of a decrypted message in accordance with the present invention;

Figure 11 illustrates an example of a display of an encrypted message in accordance with the present invention; and

20 Figures 12 and 13 are flow diagrams illustrating encryption key updating procedures carried out in accordance with the present invention.

A GSM network, referred to as a public land mobile network (PLMN), is schematically illustrated in Figure 1. This is in itself known and will not be

described in detail. A mobile switching centre (MSC) 2 is connected via communication links to a number of base station controller (BSCs) 4. The BSCs 4 are dispersed geographically across areas served by the mobile switching centre 2. Each BSC 4 controls one or more base transceiver stations (BTSS) 6 located remote from, and connected by further communication links to, the BSC. Each BTS 6 transmits radio signals to, and receives radio signals from, mobile stations 8 which are in an area served by that BTS. That area is referred to as a "cell". A GSM network is provided with a large number of such cells, which are ideally contiguous to provide continuous coverage over the whole network territory. The radio signals are separated into a number of distinct communications channels. These include common channels and traffic channels. The traffic channels are used for point to point communications (voice calls, data calls, etc) with specific mobile stations. The common channels are received by all mobile stations being served by the cell and contain signalling and/or message data.

The mobile switching centre 2 is also connected via communications links to other mobile switching centres in the remainder of the mobile communications network 10, and to other networks such as a public service telephone network (PSTN), which is not illustrated. The mobile switching centre 2 is provided with a home location register (HLR) 11 which is a database storing subscriber authentication data including the international mobile subscriber identities (IMSI) which are unique to each mobile station 8. An

IMSI consists of a mobile country code (3 decimal digits), a mobile network code (2 decimal digits) and a mobile subscriber code (up to 10 decimal digits) identifying a subscriber within a particular network. The IMSI is also stored in the mobile station in a subscriber identity module (SIM) (to be described below) along with other subscriber-specific information.

The mobile switching centre is also provided with a visitor location register (VLR), not shown, which is a database temporarily storing subscriber authentication data for mobile stations active in its area.

In addition, the MSC is connected to a cell broadcast centre (CBC) 12 for originating cell broadcast (CB) messages in the network, a short message centre (SMC) 13 for handling the transfer of point to point short messages within the network, a network management centre (NMC) 14 for performing management functions in the network, and a customer services system (CSS) 15 for performing customer service functions, including the updating of customer subscription data for example by manual input at workstations in the system.

Referring to Figure 2, a mobile station 8, more specifically a cellular mobile telephone, comprises a transmit/receive aerial 16, a radio frequency transceiver 18, a speech coder/decoder 20 connected to a loudspeaker 22 and a microphone 24, a processor circuit 26 and its associated memory 28, an LCD display 30 and a manual input port (keypad) 32. The mobile station 8 is connected to a removable SIM 34 via electrical contacts 35.

The SIM 34 connected to the mobile station has a SIM processor 36, for example a Hitachi H8 microprocessor, and SIM memory 38, which includes for example 16 kilobytes of mask-programmed ROM 38a containing the SIM operating system, 8 kilobytes of read/write EEPROM 38b for the non-volatile storage of data items and 256 bytes of RAM for use by the SIM processor 36 during operations.

As described above, the SIM 34 is used for the storage and retrieval of data items by the processor 26 of the mobile station 8. The command set, data file structure and data coding format for data communicated via the interface between the mobile station processor 26 and the SIM processor 36 are all specified, in GSM technical specification 11.11.

Referring back to the network elements illustrated in Figure 1, the CBC 12 holds a set of cell broadcast messages to be broadcast within the network, and transmits them to the BSCs 4 in accordance with location areas which are predefined for each message type. Each cell broadcast message is provided with a unique message identifier (a 16 bit integer), which identifies the type of the message. The BSCs 4 then proceed to broadcast the message, via the respective BTSs 6, on their CBCHs. The CBCH protocols and the timing of the broadcasts are specified in GSM technical specification 05.02.

The CBC 12 holds a list as illustrated in Figure 3, specifying encryption keys for each type of message which is to be broadcast in encrypted form. For each such message, the key is listed against the message identifier. Each key is

a 16 bit integer and, since the message identifiers are also 16 bit integers, no two keys in the list need to be the same. The keys are used to encrypt a message using an XOR function as will be described below.

5 Figure 4 illustrates a procedure carried out by the CBC 12 when receiving a new message for transmission as a cell broadcast message. A new message may be provided in the CBC 12 for example by manual input on a workstation associated with the CBC, or may be provided on-line from a remote source.

10 When the CBC 12 receives the new message, which may be an update of a previous message stored for the same message identifier, the message is stored by the CBC 12 and any previous message stored for the same message identifier is overwritten, step 50.

15 Next, the CBC 12 checks, using the message identifier provided with the new message, whether the message identifier appears in the key list illustrated in Figure 3. If no key is held for that particular message identifier, the message will be made generally available by cell broadcast to all mobile stations served in the cells in which the message is to be distributed. The message is transmitted for broadcast to the relevant BSCs 4 in unencrypted form, step 52.

20 The cell broadcast message may consist of one or more (up to a maximum of 15) pages. Each cell broadcast page consists of 88 octets of information, consisting of a 6 octet header and 82 octets for message text. A 7 bit default character set is used, equating to up to 93 characters per page.

Figure 5 illustrates the manner in which each page of a cell broadcast message is transmitted in a cell by the BSC/BTS on the CBCH. The broadcast is divided into four blocks per page. The first block 100 contains 2 octets of data 108 indicating the serial number for the page, 2 octets of data 110 indicating the message identifier for the page, 1 octet of data 112 identifying the coding scheme used for the message text, and 1 octet of data 114 indicating the page parameter. The remaining 16 octets of data 116 contain the first part of the message text for the page.

The remaining 3 blocks 102, 104, 106 of the page broadcast consists entirely of message text, except each block is headed by a single octet of data 118 indicating the block type.

The serial number indicated in block portion 108 is a 16 bit integer which is used to identify a particular message. The serial number is updated when a message with a given message identifier is updated. The serial number consists of a 12 bit message code and a four bit update number, which are incremented according to message updates.

The message identifier in portion 110 is used to identify the type of message, as described above.

The coding scheme indicated in portion 112 is used to indicate the source language of the message, allowing a user to screen out any messages received in a language in which they are not conversant. The page parameter

indicated in portion 114 is used to specify the current page number within a message and the total number of pages within the message.

5 The message text for each page consists of up to 93 characters. If the message text within a page is shorter than 93 characters in length, the carriage return (CR) character is used to provide packing, thus bringing the total number of characters to 93. To maintain an integral number of octets, the remaining 5 bits are set to "0" as padding data at the end of the page.

10 The block structure illustrated in Figure 5 is that of a conventional cell broadcast message, and may be received and displayed by currently-available GSM-type mobile stations in receipt of the cell broadcast channel on which the message is broadcast.

Referring again to Figure 4, if on the other hand the CBC 12 detects the message identifier of the new message in the key list, the corresponding key is retrieved, step 54. The key is then used to encrypt the message, step 56, which is then transmitted to the appropriate BSCs 4, step 58. The encryption of step 56 is performed by applying an XOR function between the most significant 8 bits of the key and each odd-numbered message text octet in a page, and by applying the XOR function between the least significant 8 bits of the key and each even-numbered message text octet in a page, except the last such octet.

20 The pages broadcast by the BSCs 4 when receiving encrypted cell broadcast messages are of the form illustrated in Figure 6. Each page consists of the same components as the unencrypted page illustrated in Figure 5, namely

4 blocks each containing the various header portions. However, the majority of the message text is encrypted, as indicated by shading in Figure 6. The last octet of each page of message text, which contains the 5 bits of padding data, is left unencrypted, in order to protect the integrity of the padding data, which would be lost if encrypted. Each of the header portions is also transmitted in unencrypted form, to allow the proper reception and reading of the data in the header portions by all mobile stations 8.

In order to properly receive and present an encrypted cell broadcast message in intelligible form to a user, a mobile station 8 must be provisioned with the decryption key corresponding with the encryption key used to encrypt the message. With the XOR function as the encryption function, the encryption/decryption process is symmetric, and the same key used to encrypt the message is used to decrypt the message. This key is referred to herein as an encryption key when to be used to encrypt data, and a decryption key when to be used to decrypt data.

In order to provision the mobile station 8 with the decryption key, a remote provisioning procedure is used, involving a remote SIM updating (RSU) message being transmitted to the mobile station 8, such as described in European patent application no. EP-A-0562890, the contents of which are incorporated herein by reference, or using the "data download via SMS Point-to-point" (SMS-PP data download) procedure as described in GSM Technical Specification 11.14, "Specification of the SIM Application Toolkit for the

Subscriber Identity Module - Mobile Equipment (SIM-ME) Interface". The decryption keys are transmitted using a point-to-point data transfer protocol, such as the GSM-defined Short Message Service (SMS), over the radio interface to the mobile station 8 for storage in the SIM 34. The SIM 34 is provided with a cell broadcast decryption keys data field dedicated to the storage of cell broadcast decryption key data.

Figure 7 illustrates the procedures carried out by the NMC 14 in order to provision the mobile station 8 of a particular subscriber with decryption keys for each limited-access message type which the subscriber is entitled to have access to. The CSS 15 holds a record for the subscriber, indicating the access rights for that subscriber. These access rights are indicated by including in the subscriber record a list of the appropriate message identifiers for the message types which the subscriber should have access to. This access rights list may be updated and changed in the CSS 15.

In order to provision the mobile station 8 of the subscriber, the NMC 14 first interrogates the CSS 15 to determine the message access rights which are held for the subscriber, step 60. The NMC 14 also interrogates the HLR 11 in order to retrieve the IMSI of the subscriber, step 62. The NMC 14 also interrogates the CBC 12 to retrieve the decryption keys corresponding to each of the message identifiers indicated in the access rights details returned by the CSS 15, step 64. Next, each of the decryption keys returned by the CBC 12 is then itself encrypted by applying the XOR function between the 16 bits of the

decryption key and 16 predetermined bits of the subscriber's IMSI record, step 66. This is to ensure that the decryption key may only be used by a mobile station 8 having access to the subscriber's IMSI (which is stored in the subscriber's SIM 34).

5 Once the decryption keys are encrypted, the NMC 14 forwards an RSU message to the SMC 13 for transmission, via the radio interface, as an SMS message to the mobile station 8 of the subscriber. The SMS message is transmitted conventionally, via a dedicated data channel, to the mobile station 8. The RSU message has the form illustrated in Figure 8, and includes a header
10 portion 70, the message identifiers for each message type to which the subscriber should have access to, the encrypted decryption keys, and alpha tags (alphanumeric identifiers) for use by the subscriber to readily identify each of the message types. The header portion 70 includes a flag indicating that the SMS message is an RSU message, and a command indicating that the contents
15 of the message are to be stored in the cell broadcast decryption keys data field.

 On receipt of the SMS message, the mobile station forwards it for storage as an SMS message to the SIM 34. However, since the message has an RSU flag, the SIM processor 36 notes that the message is an RSU message, and updates the cell broadcast decryption keys data field in the SIM 34 with the
20 message identifiers, the corresponding encrypted keys, and the corresponding alpha tags contained in the RSU message. The mobile station is now provided with the capability to decrypt all encrypted cell broadcast messages having

message identifiers corresponding to those stored in the cell broadcast decryption keys data field.

5 A user of the mobile station may, by appropriate keystrokes on the keypad 32, select cell broadcast messages which the mobile station is to pick up and store for possible display by the user. The user may display the alpha tags for the message types of limited access messages, in order to aid the selection of the limited access message types which the user wishes to have displayed. The user is also able to select the message identifiers for message types of general access messages, and for message types of limited access messages which the
10 mobile station has no decryption keys.

When a cell broadcast message is received by the mobile station 8 which has a message identifier of the type selected for possible display by the user, and no message is yet stored for the message identifier, the mobile station 8 picks up the message and stores the message in a cell broadcast message data field
15 provided in the SIM 34. If the SIM 34 already has a message stored for the message identifier in the cell broadcast message, the mobile station 8 checks the serial number of the message to determine whether it has been updated. If so, the mobile station overwrites the previously-stored message in the SIM 34 with the updated message. Otherwise, the mobile station 8 ignores the contents of
20 the cell broadcast message.

When a cell broadcast message is newly picked up and stored, the user is prompted, for example by an audio tone or by a particular icon on the LED

display 30 of the mobile station 8, to indicate that a cell broadcast message is ready to be displayed. The mobile station then performs the procedures illustrated in Figure 9.

5 The mobile station first waits for input by the user requesting the message to be displayed. On receipt of such input, the mobile station checks whether it is currently camped on its home network (HPLMN). If the mobile station is camped on a network which is not its home network, the mobile station proceeds directly to display the stored message. If the message is encrypted, the encrypted message is displayed in a form unintelligible to the
10 user, step 78, as the message is of the limited access type and access to the information is denied to the subscribers of other networks. If the message however is unencrypted, i.e. of the general access type, the message is displayed in an intelligible form, step 80.

If the mobile station is camped on its home network, the mobile station
15 checks whether the SIM 34 has the cell broadcast decryption keys data field provided in accordance with this invention. If not, the mobile station proceeds once again to either display an encrypted message, step 78, or an intelligible message, step 80, depending on the access type of message broadcast.

If the SIM 34 currently in the mobile station does have the cell broadcast
20 decryption keys data field, the mobile station proceeds to interrogate the SIM 34 to check whether the message identifier of the stored message is present in the cell broadcast decryption keys field. If not, the message received may be of a

general access type, and the message is displayed by the mobile station 8 in intelligible form, step 80. Otherwise, the message is of a limited access type to which the user has no access rights. The message is then displayed by the mobile station 8 in encrypted, i.e. unintelligible form, to prevent receipt of the information in the message by the user, step 78.

If the message identifier of the stored message is present in the cell broadcast decryption keys data field on the SIM 34, the mobile station 8 proceeds to retrieve the encrypted decryption key corresponding to the message identifier of the stored message, along with the subscriber's IMSI, from the SIM, step 82.

With the encrypted decryption key and the IMSI, the mobile station 8 performs the reverse of the encryption process carried out in the NMC 14, to obtain the original decryption key, step 84. This decryption is carried out by performing an XOR function between the 16 bits of the encrypted decryption key and the same set of 16 predetermined bits from the subscriber's IMSI used in the encryption process.

The mobile station 8 then proceeds to decrypt the stored message, by performing the reverse of the encryption process carried out in the CBC 12 when generating the encrypted cell broadcast message. Namely, the mobile station performs the XOR function between the 8 most significant bits of the decryption key and each odd-numbered message text octet, and between the 8 least significant bits of the decryption key and each of the even-numbered

message text octets, except for the last octet in each page (which was originally not encrypted). This returns the original cell broadcast message text, which is then displayed on the LCD display 30 of the mobile station, step 88, in a form intelligible to the user.

5 Figure 10 illustrates an example of an original cell broadcast message, consisting of one page containing 89 message text characters and 4 carriage return (text padding) characters. This message is encrypted as described in relation to Figure 4, and after receipt and storage by the mobile station may be displayed in accordance with the procedure shown in Figure 9.

10 If the mobile station has been provisioned with the corresponding decryption key, the message may be displayed in its original form as illustrated in Figure 10.

 If however the mobile station has not been provisioned with the appropriate decryption key, the message will appear as illustrated in Figure 11,
15 as a pseudo-random character set.

 Because the number of bits of the encryption key is not equal to, nor a multiple of, the number of bits used per character in coding the text, there is no direct correspondence between any one of the original characters and the characters displayed in the encrypted text. In this case, the coding scheme used
20 for the text characters utilises 7 bits per character, and the encryption keys contain 16 bits. Of course, other combinations of text character coding length and encryption key length may be used to similar effect.

To ensure the long-term security of the encryption method used for limited access messages, the encryption keys used to encrypt the message texts will periodically be altered. Figure 12 illustrate a procedure carried out by the CBC 12 to update a particular encryption key. The CBC 12 first randomly generates a new 16 bit encryption key, step 90, and overwrites the previously-stored encryption key in the list illustrated in Figure 3 for the message identifier in question, step 91. Next, the CBC 12 proceeds to retrieve the message previously stored for the message identifier in question, step 92, and proceeds to encrypt the message with the newly generated encryption key, step 93. This encryption process is identical to that carried out when the message was originally received by the CBC 12 as described in relation to Figure 4, of course using a different encryption key. Once the message is encrypted, the new cell broadcast message is forwarded to the appropriate BSCs 4, step 94, for broadcast by the BTSs 6 on their CBCHs to mobile stations 8 receiving the cell broadcast channel in the cells served by the BSCs 4 in question.

Once a new encryption key has been generated in the CBC 12, and the corresponding cell broadcast message has been encrypted with the newly-generated key, the mobile stations 8 of users having access rights to the same message type must be provisioned with the new decryption key.

The first step of provisioning the mobile stations 8 of the appropriate subscribers with new decryption keys generated in the CBC 12 is the procedure carried out in Figure 13. First, the CSS 15 receives from the CBC 12 a list of

message identifiers for the messages for which the decryption keys have been updated, step 95. The CSS 15 then proceeds to search its store of subscription records for the message identifiers on the updated decryption keys list, in order to determine which subscriptions require updated decryption keys, step 96. The
5 CSS 12 then constructs a list of such subscriptions, which are forwarded to the NMC 14 to allow the NMC 14 to perform the appropriate provisioning procedures, step 97. The NMC 14 then proceeds to perform the procedure described in relation to Figure 7 for each subscription appearing on the list received from the CSS 15. This results in the mobile stations of each such
10 subscription receiving a new RSU message containing updated decryption keys, in encrypted form, for message types to which the subscriber has access. These decryption keys are suitable for use in decrypting messages encrypted with the newly-generated encryption keys.

The encryption/decryption mechanism utilised in the above-described
15 embodiment utilises the two-way encryption/decryption character of the XOR function, and is sufficiently secure for use in relation to many types of information. However, it will be appreciated that other two-way encryption/decryption mechanisms, for example using symmetric or public/private encryption/decryption keys, may be utilised to provide more (or less) secure
20 encryption/decryption mechanisms.

In the above-described embodiment, the general-access messages are not subject to the XOR function used in the encryption/decryption process.

However, it would also be possible to subject the message to the XOR function using a "free" key of the form of 16 bits of "0", which results in a message coding which is identical to the original message coding. This XORing with the "free" key may be performed in the CBC 12 when "encrypting" a general access message, and/or by the mobile station 8 when "decrypting" a general access message. In effect, no encryption or decryption would take place.

In the above-described embodiment, the mobile station 8 performs the decryption of the cell broadcast message text. This requires the mobile station itself to be customised, in relation to currently existing mobile station types, in order to allow the mobile station to present the encrypted cell broadcast messages in plain text form. In a further embodiment, a standard mobile station, such as a GSM (Phase 2+) mobile station supporting the SIM Toolkit as described in GSM Technical Specification 11.14, may be used. In this further embodiment, the functionality for decrypting encrypted cell broadcast messages is contained in the SIM 34 itself, the SIM 34 being SIM Toolkit enabled.

In order to avoid repetition, it should be understood that the functionality described in relation to each of Figures 3, 4, 7, 8, 12 and 13 is intended to apply equally in relation to 13. This embodiment differs primarily from the first-described embodiment in that the special cell broadcast coding scheme illustrated in Figure 6 is not necessary, a conventional "data download via SMS-CB" coding scheme being used instead, and in that the procedure illustrated in Figure 9 is not carried out by the mobile station, the mobile station

instead passing "data download via SMS-CB" messages directly to the SIM, and subsequently being instructed by the SIM (the SIM being proactive) to display a plain text version of a cell broadcast message received in encrypted form.

5 Referring to Figure 4, in this embodiment any suitable type of encryption technique may be used in step 56. This may be the XOR function previously described, or other encryption techniques such as DES, RSA, etc.

10 In place of the coding scheme illustrated in Figure 6, in this embodiment each of the BSCs 4 broadcasting encrypted cell broadcast messages formats the encrypted message as a "data download via SMS-CB" message, the encrypted message being included in the cell broadcast page along with an identifier for the key used to encrypt the message. The cell broadcast message includes a cell broadcast message identifier, which specifies the type of content contained in the cell broadcast page, and a transfer protocol identifier indicating that the
15 message type is "SIM data download".

In addition to the field dedicated to containing decryption keys, which may be populated by means of RSU procedures as described above, the SIM 34 contains a Cell Broadcast Message Identity for Data Download (CBMID) data field, as described in GSM Technical Specification 11.11, which holds data
20 identifying the message content types the subscriber wishes the mobile station 8 to accept. Furthermore, the SIM 34 includes an application programme, which

may for example be stored in ROM or EEPROM on the SIM, for performing decryption and controlling the display of the mobile station 8.

When the mobile station receives the cell broadcast download message, the mobile station 8 first queries the CBMID data field of the SIM to determine whether the message ID received for the cell broadcast message is currently
5 selected by or for the subscriber. If a corresponding entry is found in the CBMID data field, the mobile station 8 transparently passes the cell broadcast page to the SIM 34 using a "cell broadcast download to SIM" command.

Reception of the cell broadcast download command by the SIM 34
10 causes the SIM to analyse the contents of at least a portion of the cell broadcast page, wherefrom it is determined whether the cell broadcast page contains an encrypted message. If so, the stored programme is invoked in order to decrypt the message, using the appropriate decryption key stored in the dedicated decryption keys field. Once the message is decrypted, the SIM passes the plain
15 text message to the mobile station in a "display text" command, in response to which the mobile station 8 displays the plain text message.

In addition to decrypting the encrypted message and commanding the mobile station 8 to display the plain text message, the SIM application programme may also perform other processes in response to data received in the
20 cell broadcast message, such as updating the contents of the CBMID data field to select new message types, on behalf of the subscriber, which the mobile station 8 should accept and handle.

As will be appreciated, in this embodiment, if a subscriber is not authorised to receive a limited access message in plain text form, the SIM may either not contain an appropriate decryption key for the message or may be at least temporarily configured by the network operator so as not to conduct the procedure described above. Instead of the procedure described above, the SIM
5 may act in one of a variety of alternative manners. For example, the SIM may command the mobile station 8 either to present the message to the user in encrypted form or to display an access-denied message, or may simply not any display on the mobile station, in response to a cell broadcast message containing
10 an encrypted message which is of a type nevertheless selected by the subscriber.

The functionality for the provision and processing of encrypted cell broadcast messages may thus be contained entirely within the mobile communications network and on the SIM 34, and standard (e.g. GSM Phase 2+) handsets may be used without modification.

15 It will be appreciated that various modifications and variations may be employed in relation to the above-described embodiments.

The provisioning of the mobile stations with decryption keys via the air interface, using the RSU-type short messages, has the advantage that no action is required on the subscriber's behalf in order to provision the SIM 34 of the
20 mobile station 8 with the decryption keys. However, the decryption keys, preferably encrypted using the subscriber's IMSI, or such like, as described, may be transmitted to the user by other methods, for example by mail. An

alternative functionality of the mobile station 8 would allow the encrypted decryption keys to be manually input to the mobile station for storage in the cell broadcast decryption keys data field in the SIM 34.

5 Other information access prevention mechanisms to those described above could also be employed, such as the remote enablement/disablement (for example using RSU messages) of a decryption function on the mobile station, or of the cell broadcast receiving function on the mobile station.

In the above-described embodiments, the SIM 34 is in the form of a module electrically connected to the mobile station 8. However, the SIM may
10 be embodied in an entirely separate module, such as a contactless smartcard transmitting data to and from the mobile station via a radio link.

Finally, although the above-described embodiments relate to a method and apparatus utilised in a GSM-type network, the present invention may of course be realised in other types of cellular telecommunications networks,
15 whether using TDMA, CDMA, or other types of radio interface protocols.

It is envisaged that further modifications and variations may be employed without departing from the scope of the present invention.

CLAIMS

1. A method of distributing information to users in a cellular telecommunications network comprising a mobile switching centre and a plurality of base stations transceiving in a plurality of cells of said network, said
5 method comprising:

providing a plurality of mobile stations, each of said mobile stations having an associated information access status;

broadcasting a signal on a common channel of at least one cell of said
10 network, said signal containing a limited access message in encrypted form, for general reception in said at least one cell;

enabling first mobile stations having a first information access status to decrypt and present said message to a user in unencrypted form when being served by said cell; and

15 preventing second mobile stations having a second information access status from presenting said message in unencrypted form to a user when being served in said cell.

2. A method according to claim 1, wherein said first mobile
20 stations are provided with a decryption key for said message.

3. A method according to claim 2, wherein said decryption key is held in a removable module which may be used in association with any of a plurality of mobile stations.

5 4. A method according to claim 3, wherein said message is decrypted in said removable module.

5. A method according to claim 2 or 3, wherein said signal contains padding data accompanying a portion of said message, and said portion is
10 contained in said signal in unencrypted form.

6. A method according to any preceding claim, wherein said signal comprises a header portion containing a message identifier accompanying a message and said method comprises enabling both said first and second mobile
15 stations to read said message identifier.

7. A method according to any of the preceding claims, wherein status data defining said information access status is stored in a removable module of a first mobile station.

20

8. A method according to claim 7, wherein said status data comprises a decryption key.

9. A method according to claim 8, wherein said decryption key is stored in said removable data store in encrypted form.

5 10. A method according to claim 9, wherein said decryption key is decrypted by said first mobile station using a data string specific to said removable module.

10 11. A method according to claim 10, wherein said data string is a subscriber identifier used in said cellular telecommunications network.

12. A method according to any of claims 7 to 11, further comprising transmitting said status data to said first mobile station via a radio interface in said cellular telecommunications network.

15

13. A method according to any preceding claim, wherein said signal comprises a plurality of limited access messages each having a corresponding access right,

20 said method comprising providing said mobile stations with said access rights and enabling only mobile stations having an access right corresponding to a limited access message to present said limited access message to a user when being served in said cell.

14. A method according to claim 13, comprising providing each of said first mobile stations with a selection of said access rights in accordance with a subscription held for each first mobile station respectively.

5

15. A method according to claim 13 or 14, further comprising storing encryption keys for each of a plurality of limited access message types, and encrypting each said limited access message using an encryption key in accordance with its respective message type.

10

16. A method according to any of claims 13 to 15, comprising storing a plurality of subscription records, each said subscription record comprising access right data defining said access rights.

15

17. A method according to claim 16, comprising altering said access right data for a subscription record to alter the type of limited access messages a user is able to receive intelligibly.

20

18. A method according to any preceding claim, wherein said signal contains a general access message, and wherein said method comprises enabling both said first and second mobile stations to present said general access message to a user when being served in said call.

19. A method according to claim 19, wherein said common channel is a cell broadcast channel of a GSM-type communications system.

5 20. A method according to any preceding claim, wherein alternative limited access message(s) are broadcast in cells located in different areas of said cellular telecommunications network.

21. Apparatus for receiving information in a cellular telecommunication system, said apparatus comprising:

means for storing a decryption key;

means for receiving a message broadcast on a common channel of a cell of said cellular telecommunications system; and

means for decrypting said message using said stored decryption key; and

15 means for displaying said decrypted message to a user.

22. Apparatus according to claim 21, wherein said storage means is part of a removable module.

20 23. Apparatus according to claim 21 or 22, wherein said displaying means is arranged to display a message in decrypted form when a decryption key for said message is held in said storage means, and to display said message

in encrypted form when no decryption key for said message is held in said storage means.

24. Apparatus according to claim 21, 22 or 23, wherein said
5 decryption means is part of a removable module.

25. A cellular mobile telephone according to claim 21, 22, 23 or 24.

THIS PAGE BLANK (USPTO)

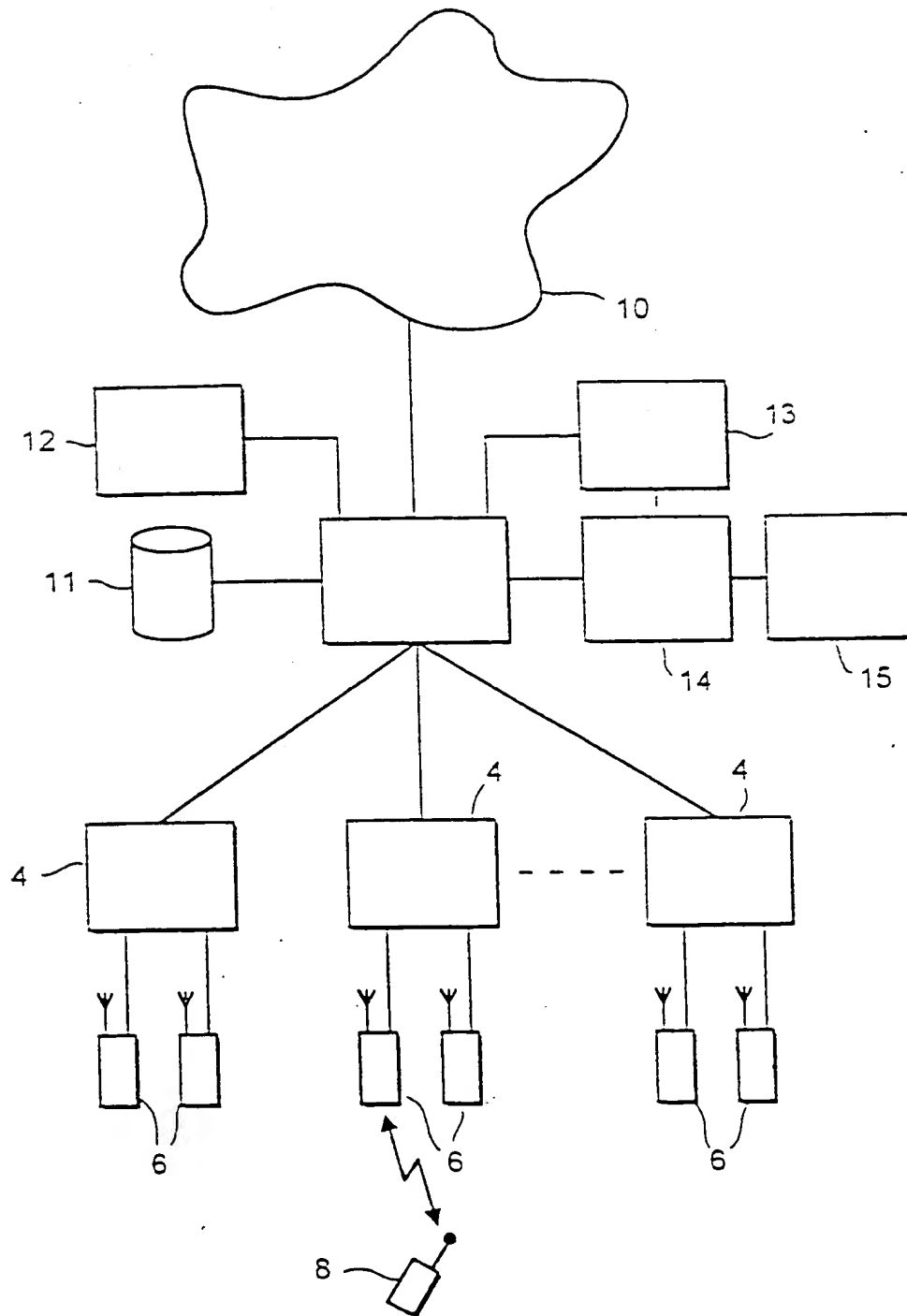


FIG. 1

420 11 90

420 11 90 PCT/PTO 1 8 JAN 2000

THIS PAGE BLANK (USPTO)

2 / 8

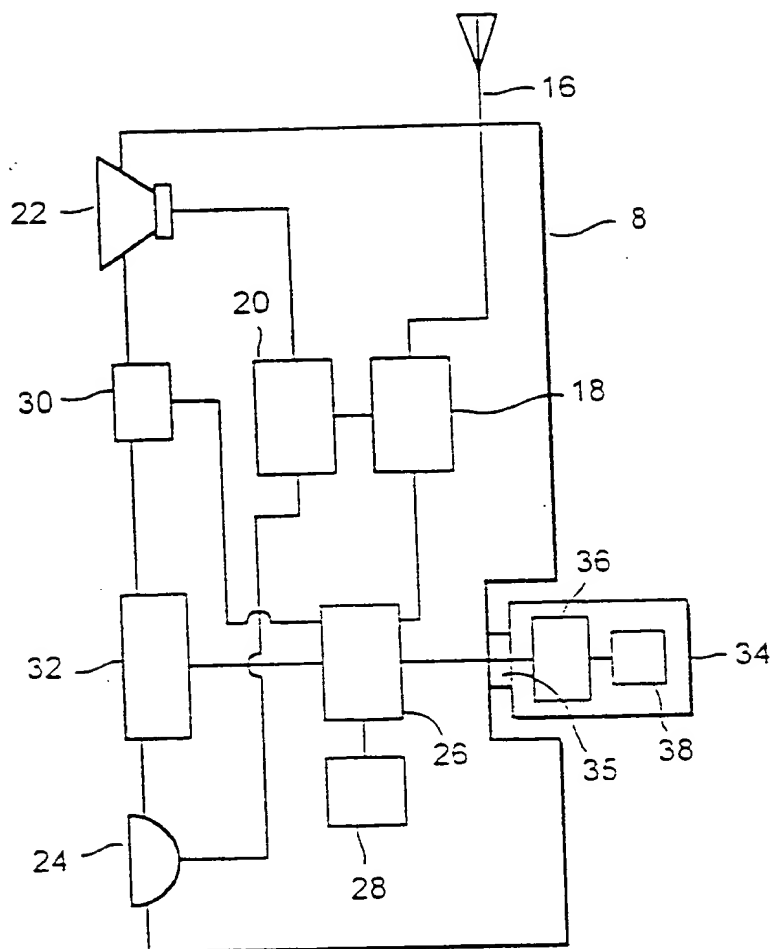


FIG. 2

MESSAGE IDENTIFIER	KEY
-----	-----
-----	-----
⋮	⋮
-----	-----

FIG. 3

3477-1-1-90

420 PCT/PTO 1 8 JAN 2000

THIS PAGE BLANK (USPTO)

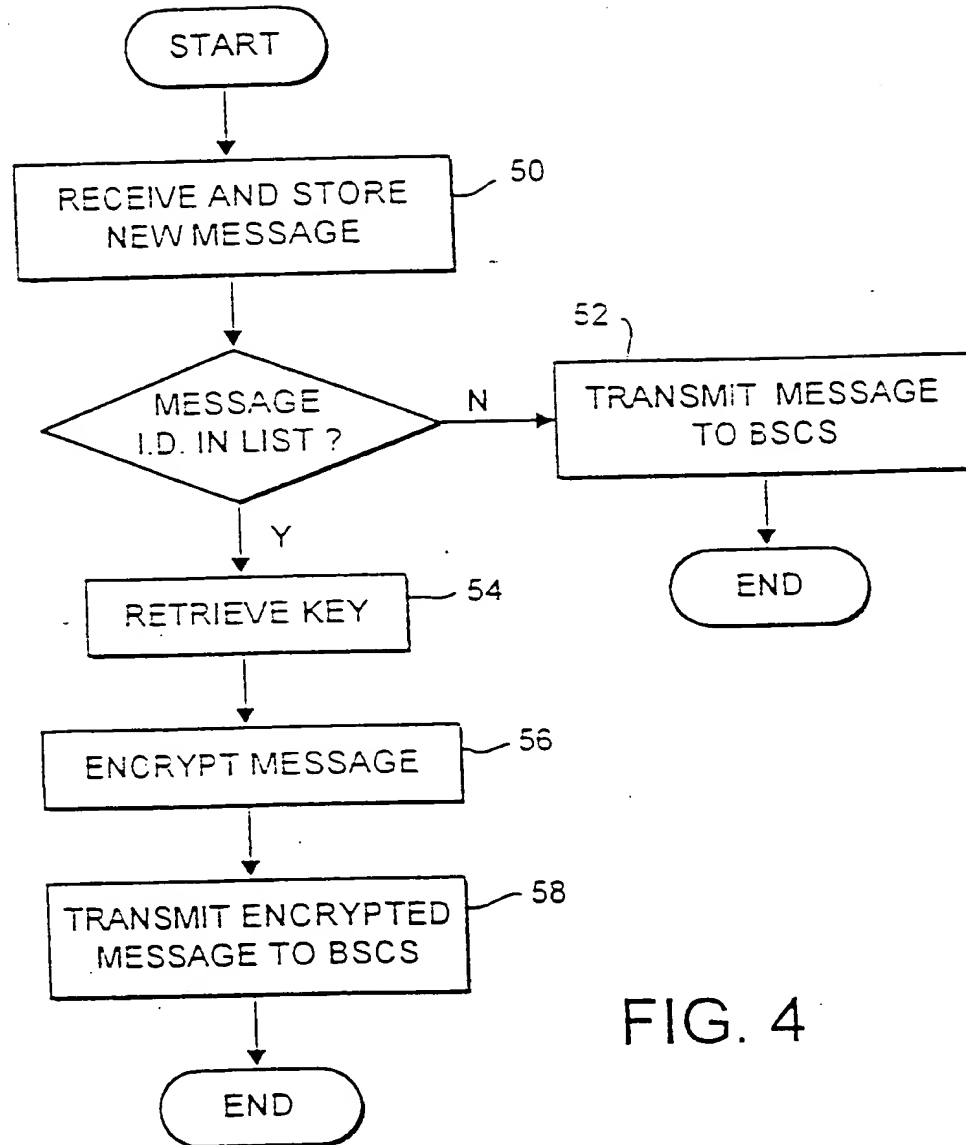


FIG. 4

337-84140

423 PCT/PTO 18 JAN 2000

THIS PAGE BLANK (USPTO)

4 / 8

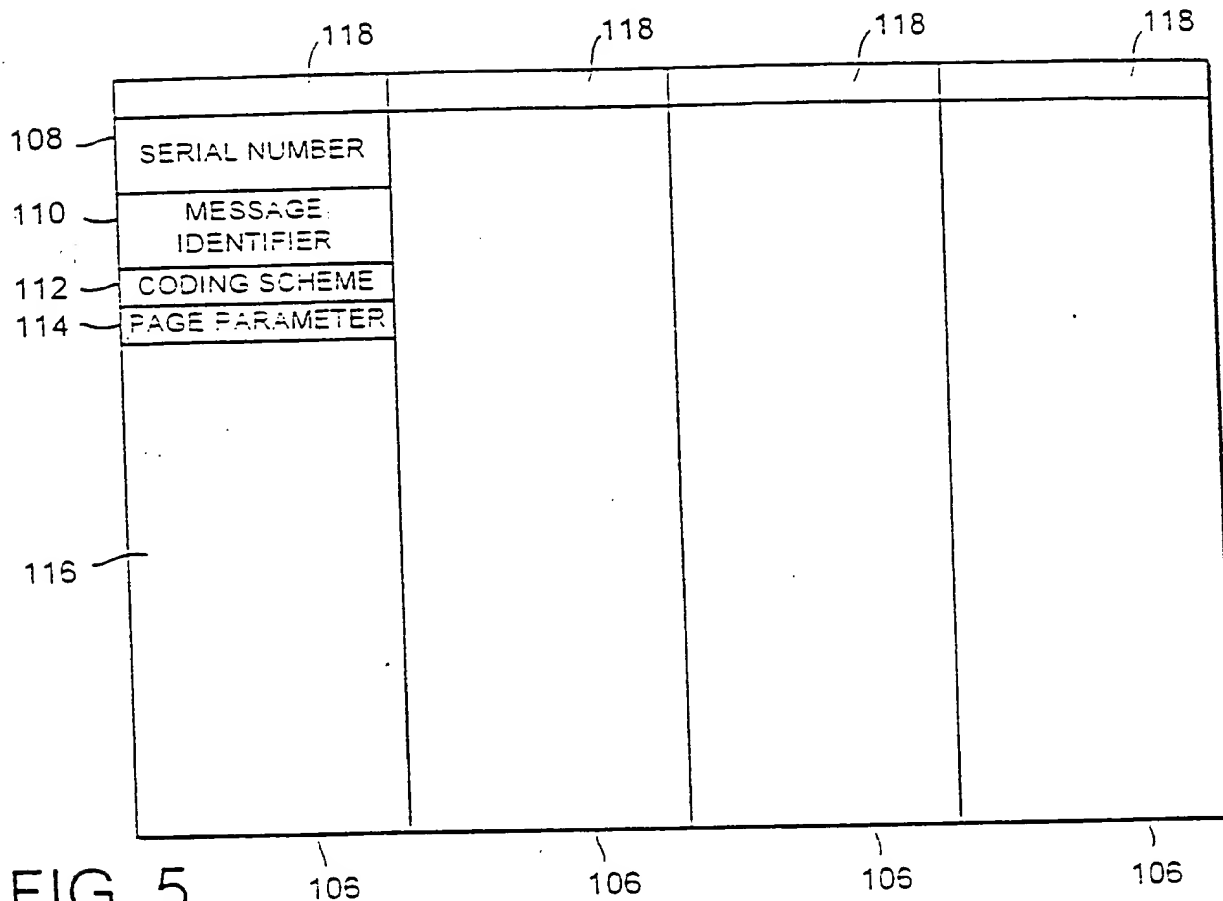


FIG. 5

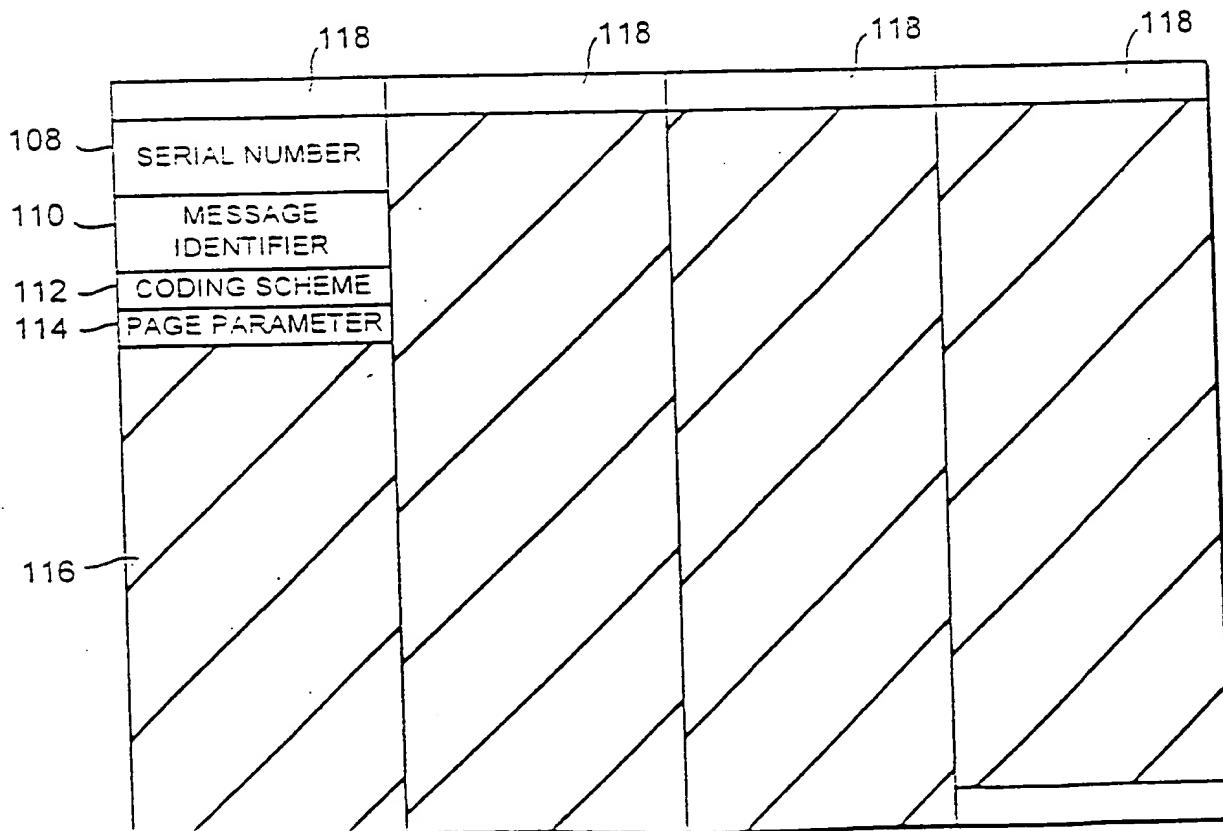


FIG. 6

420 4A 90

420 4A 90 PCT/PTO 18 JAN 2000

THIS PAGE BLANK (USPTO)

5 / 8

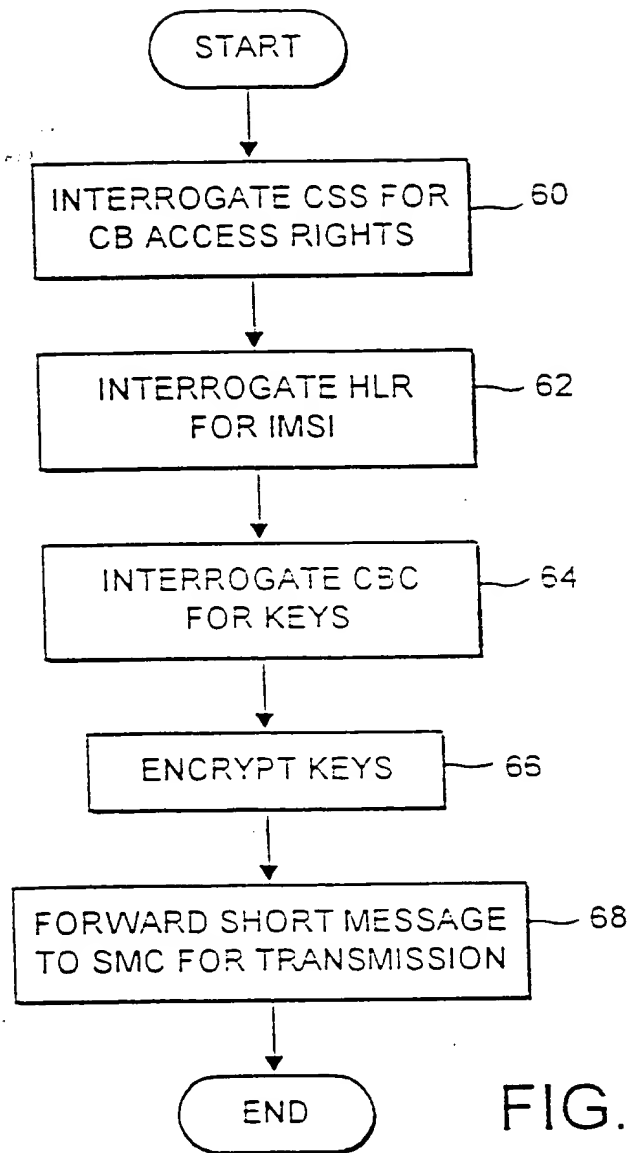


FIG. 7

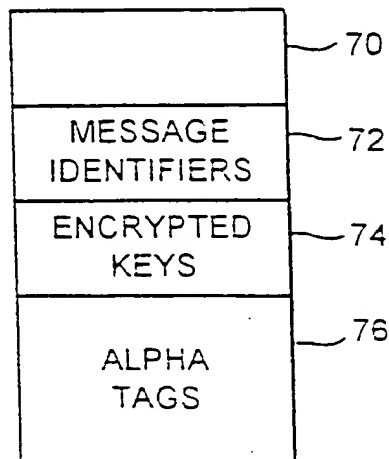


FIG. 8

423 ● c'd PCT/PTO 1 8 JAN 2000

THIS PAGE BLANK (USPTO)

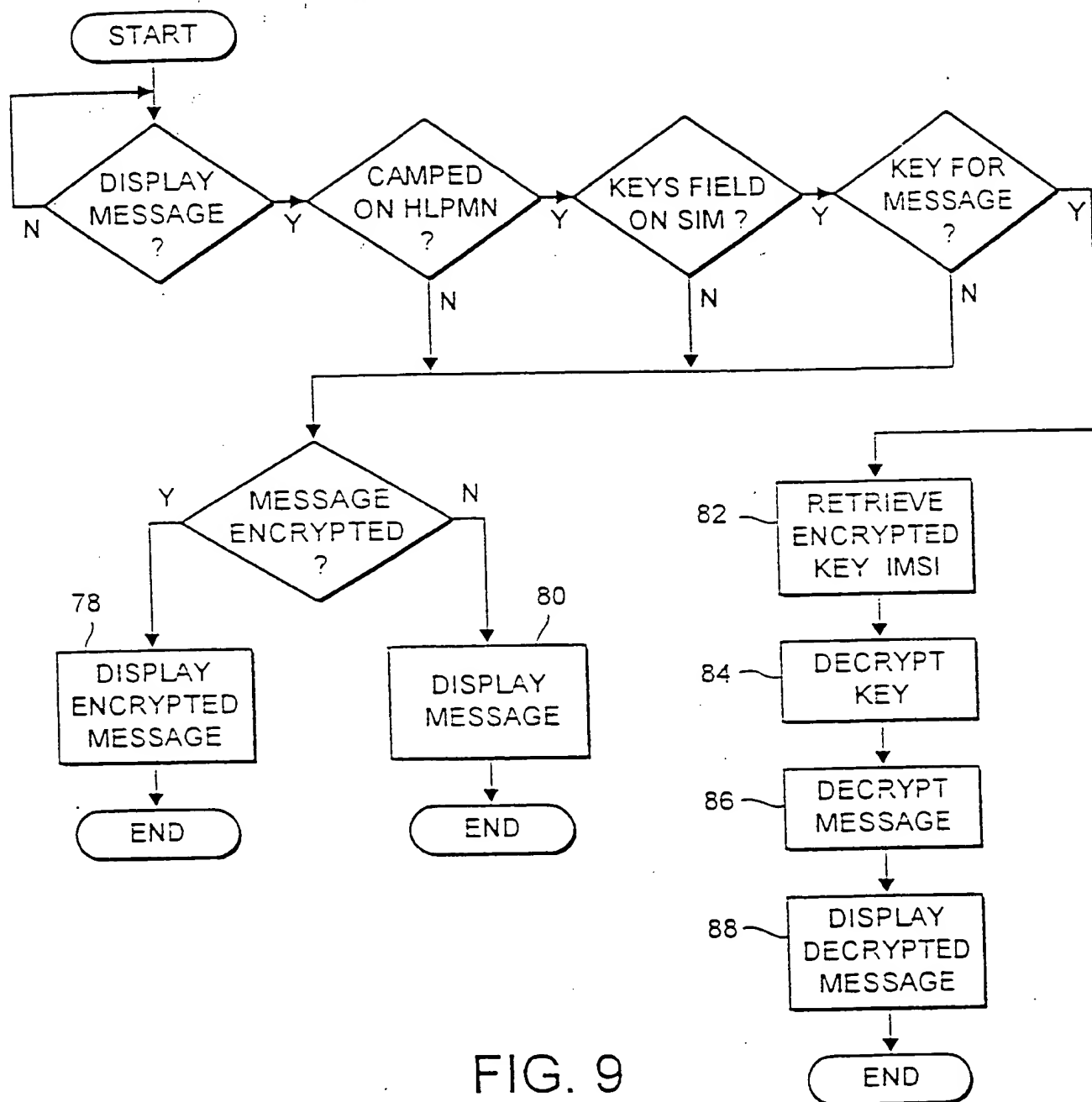


FIG. 9

423 Rec'd PCT/PTO 18 JAN 2000

THIS PAGE BLANK (USPTO)

T	h	i	s		i	s		a	n		e	x	a	m	p	i	e		o	f		h	o	w		S	M	S	I
C	B		m	e	s	s	a	g	e	s		s	h	a	i	i		b	e		c	o	d	e		C	a		CR
I		"	0	4	5	4	6	2	4	8	2	3	"		F	o	r		m	o	r	e		i	n	f	o		
CR	CR	CR																											

FIG. 10

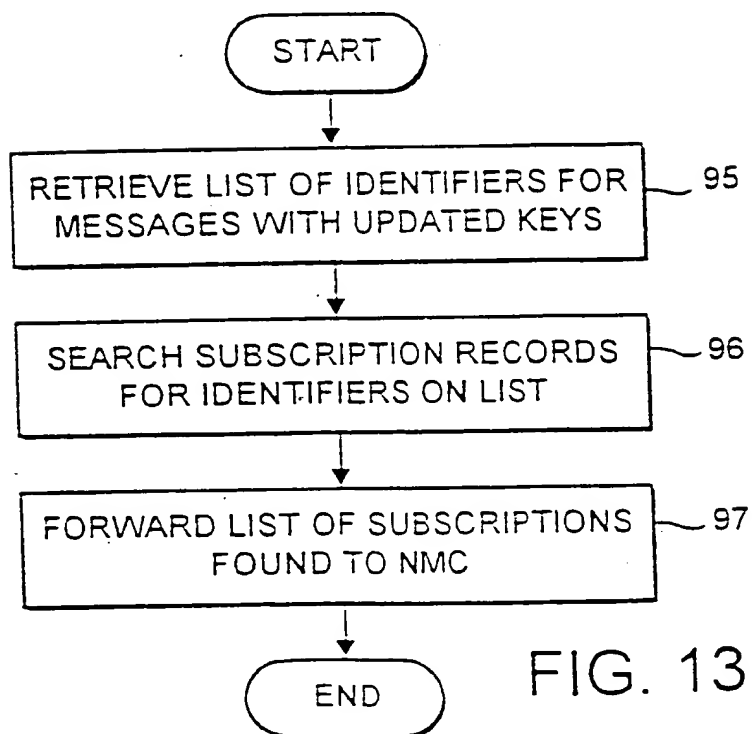
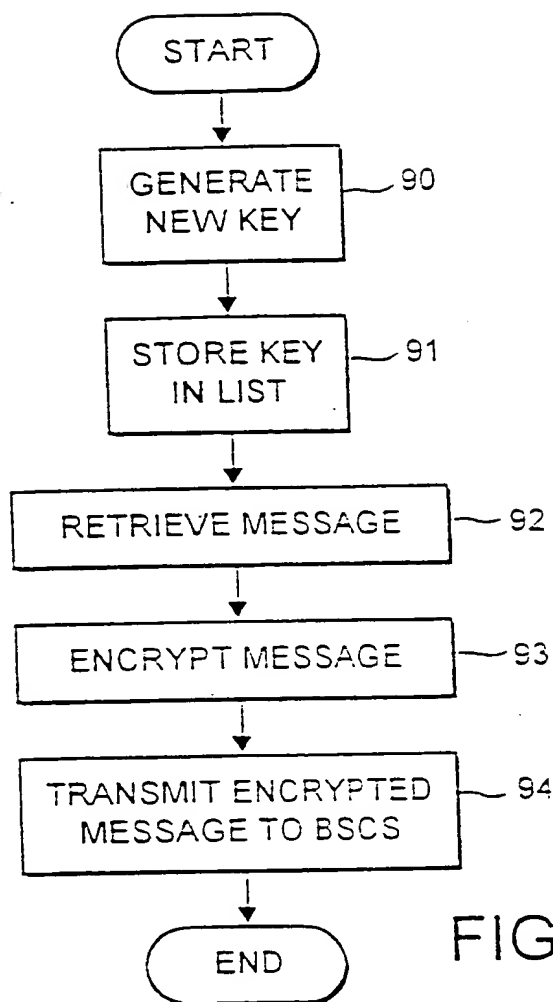
U	s	Ü	æ	ö	P	@	F	.	u	"	φ	□	X	β	U	I	ü	"	ψ	£	:	0	N/U	ç	:	:	d	#	á	0
0	□	m	v	R	æ	/	X	Δ	¥	>	:	F	ü	=	ö		6	/	ü	ü	ü	CR	3	N	Δ	\$	b	X	V	\$
0	0	Q	V	y	0	¥	X	n	CR	K	V	ü	9	"	ó	3	K	S	φ	φ	"	I	R	N	5	W	Ω	ç	C	II
:	c	\$																												

FIG. 11

423 Recd PCT/PTO 1 8 JAN 2000

THIS PAGE BLANK (USPTO)

8 / 8



486 Rec'd PCT/PTO 1 8 JAN 2000

THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

International Application No.

GB 98/02064

A. CLASSIFICATION OF SUBJECT MATTER
 IPC 6 H0407/22 H0407/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 H040

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 96 41493 A (ERICSSON TELEFON AB L M) 19 December 1996	1,2,6, 13-16, 18-21,25
Y	see page 40, line 5 - page 41, line 2 see page 52, line 20 - page 53, line 17 see page 55, line 10 - line 17 see page 57, line 19 - page 58, line 6 see claims 1-10 --- -/--	3,7,8, 12,17,22

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

10 November 1998

Date of mailing of the international search report

18/11/1998

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040. Tx. 31 651 epo nl.
 Fax: (+31-70) 340-3016

Authorized officer

Baas, G

INTERNATIONAL SEARCH REPORT

Patent Application No.

PCT/GB 98/02064

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication where appropriate, of the relevant passages	Relevant to claim No.
Y	FARRUGIA A J ET AL: "SMART CARD TECHNOLOGY APPLIED TO THE FUTURE EUROPEAN CELLULAR TELEPHONE ON THE DIGITAL D-NETWORK" SELECTED PAPERS FROM THE SECOND INTERNATIONAL SMART CARD 2000 CONFERENCE, 4-6 OCTOBER 1989, AMSTERDAM, NL, 1 January 1989, pages 95-107, XP000472724 see page 100, line 1 - page 103, line 21 ---	3,7,8, 12,22
Y	US 5 371 493 A (SHARPE ANTHONY K ET AL) 6 December 1994 see column 3, line 3 - line 10 see column 6, line 35 - line 42 ---	17
A	EP 0 689 368 A (PTT GENERALDIREKTION) 27 December 1995 -----	

INTERNATIONAL SEARCH REPORT

information on patent family members

International Application No

PCT/GB 96/02064

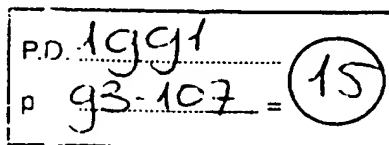
Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 9641493	A	19-12-1996	US 5768276 A	16-06-1998
			AU 6020296 A	30-12-1996
US 5371493	A	06-12-1994	DE 69219991 D	03-07-1997
			DE 69219991 T	27-11-1997
			EP 0538933 A	28-04-1993
			JP 5218946 A	27-08-1993
			SG 48347 A	17-04-1998
EP 0689368	A	27-12-1995	AT 153206 T	15-05-1997
			AU 691271 B	14-05-1998
			AU 2174595 A	04-01-1996
			BR 9508091 A	12-08-1997
			CA 2152215 A	21-12-1995
			WO 9535635 A	28-12-1995
			CN 1128476 A	07-08-1996
			CZ 9603513 A	14-05-1997
			DE 59402759 D	19-06-1997
			DK 689368 T	08-12-1997
			ES 2103557 T	16-09-1997
			FI 965078 A	17-12-1996
			GR 3023908 T	30-09-1997
			HU 76397 A	28-08-1997
			JP 8265843 A	11-10-1996
			NO 965315 A	18-02-1997
			NZ 287390 A	19-12-1997
			PL 317643 A	14-04-1997
			SG 34235 A	06-12-1996
			SI 9520064 A	30-04-1997
			SK 161396 A	05-11-1997
			ZA 9505091 A	10-04-1996

THIS PAGE BLANK (USPTO)

XP 000472724

Smart Card 2000
D. Chaum (Editor)
© 1991 Elsevier Science Publishers B.V. All rights reserved

00007 325
70467:3252
93-107



Smart Card Technology Applied to the future European Cellular Telephone on the digital D-Network

A.J. Farrugia^a and P. Peyret^b

^a GEMPLUS CARD International, Avenue du Pic de Bertagne, Parc d'activités de la plaine de Jouques. PO Box 100 13881 GEMENOS Cedex.

I. ABOUT THIS DOCUMENT

This document is an overview of the application of smart card technology as used in the Subscriber Identity Modules of the future European mobile cellular telephone system based on the digital D-network.

It is not an official document and, as such, does not involve the responsibility of official bodies whatsoever.

This document is the property of GEMPLUS Card International. It must not be copied partly or in full without obtaining the prior written consent of GEMPLUS.

II. BACKGROUND

The task of specifying and standardizing a cellular mobile-phone system using digital RF transmission within the 900-MHz band has been undertaken in Europe in the early eighties. Since then, the work done by the CEPT¹, which was later to become the ETSI², has covered the description of potential services, as well as the functions of the system, the interfaces between the system components, including the RF characteristics, and has led to a coherent set of technical recommendations.

Because the working group was known as the "Groupe Spécial Mobiles", such systems as described in the set of recommendations are designated as GSM systems.

The GSM recommendations make use of advanced technologies in many aspects of the system:

- full-digital RF transmission with low bit-rate coding
- ISDN-type layered protocols in the networks
- CCITT N°7 protocol handling between networks

¹ CEPT = Conference Européenne des postes et telecommunications

² European Telecommunications Standards Institute

This extensive work has paved the way to the agreement, reached in 1987 in Copenhagen, by 15 european network operators, to implement jointly a GSM system by 1991.

Such a european-wide system will be comprised of several Public Land Mobile Networks (PLMN), each PLMN operator covering one or several geographical areas. Any customer having subscribed to the relevant services available from his home PLMN, will be able to travel throughout Europe with his mobile equipment, and make phone calls or access any telecommunication services from any area covered by a PLMN of the GSM system, while being billed on his home account. Also, the travelling user will be able to rent or borrow a GSM mobile phone abroad while still retaining the capability of being reachable at his usual number.

Being capable of accommodating the "roaming" user, as described above, implies a noticeable feature of the GSM system: a GSM system requires a reliable yet flexible way of uniquely identifying each single customer throughout the entire span of the inter-connected networks. Also, it is required that the identity of a customer be not attached to a particular phone station. Thus, the concept of a detachable Subscriber Identity Module (SIM) has been adopted.

A Subscriber Identity Module Expert Group (SIMEG) has been formed to study this particular point. The SIMEG has specified the application of Smart (microprocessor-based) Card technology to implement the GSM Subscriber Identity Modules.

GEMPLUS has been a leading member of the SIMEG group of experts since its creation, and has played a key-role in the drafting and writing of the SIM specification.

GEMPLUS is the first company to offer commercial samples of Smart Cards, smart card chip Modules, and Plug-In SIMs, complying to the SIM specification.

III. THE GSM SYSTEM

A. Definitions

The "Groupe Spécial Mobile" has generated a great deal of documents describing extensively the elements included in a GSM network. A specific vocabulary is being used in those documents to define unambiguously the components involved in each part of the system.

Not all the components need to be known by the reader of this paper; however, the following list is useful for anyone not yet familiar with the system:

1. Public Land Mobile Network (PLMN)

The PLMN designates an homogeneous part of the cellular phone network operated by one entity such as an Operator (or Consortium of Operators).

For example, a subscriber will have a Home PLMN, covering the geographical area of his main residence, the operator of which he is likely to get his subscription from. When travelling abroad, he may access services through other PLMNs.

2. Mobile Station (MS)

The MS is the functional element which allows the subscriber to access the telecommunication services.

Depending on the type of services it provides access to (e.g. vocal only or vocal + non-vocal), and depending on the characteristics of its RF part (such as range), a Mobile Station can be of one of three types:

- "car" station: to be installed in a vehicle
- "portable" station: can be moved around when necessary
- "pocket" or "hand-held" station: small enough to be carried around at all times

3. Mobile Equipment (ME)

The part of the Mobile Station excluding the Subscriber Identity Module

4. Subscriber Identity Module (SIM)

The removable part of the MS which contains the information related to the Subscriber. It is physically and logically distinct from the rest of the station.

Two physical implementations can exist:

- "Card" SIM, which has the same dimensions as a credit card and complies to the ISO IS 7816-1, -2 for the physical layout.
- "Plug-In" SIM which is smaller than a credit card, hence is best suited for portable and pocket stations. The Plug-In SIM is installed semi-

permanently inside a station, i.e. it is not meant to be inserted and removed upon each transaction.

5. Base Transceiver Station (BTS)

The Base Transceiver Station is in charge of transmitting and receiving locally the RF signals to and from the Mobile Stations located in its area of coverage. BTSs are scattered all over the PLMN territory to provide the necessary coverage.

6. Base Station Controller (BSC)

The Base Station Controller is in charge of controlling a group of BTSs. The link between the BSC and the BTSs it controls, is separate from the RF link between the BTSs and the MSs.

7. Mobile service Switching Center (MSC)

The Mobile service Switching Center handles the switching functions of the PLMN.

The MSC interfaces the cellular network with other switched or packet networks. For example, 4 mobile voice transmissions of 13 Kb/s each can be fitted into one 64 Kb/s channel of another network.

8. International Mobile Subscriber Identity (IMSI)

A mobile subscriber of the GSM system is uniquely identified by its IMSI code, which is an individual number permanently attached to him. The IMSI code enables the system to identify the country and PLMN of origin of the user, as well as identify the Home Location Register (see below) data-base and record address in the data base for that particular customer. The IMSI is not used as an addressing means, except for a few rare cases. It is kept in a secure memory in the SIM.

9. Temporary Mobile Subscriber Identity (TMSI)

In order to keep the subscriber identity confidential, the IMSI code is replaced as often as possible with the Temporary Mobile Subscriber Identity code, which is only valid within the geographical area where the mobile is located; Furthermore, the TMSI is replaced upon each location up-dating, so as to prevent an intruder from discovering and making use of the correspondence between the TMSI and the IMSI.

10. Location Area Identification (LAI)

The Location Area Identification is the data which identify to the network where the mobile subscriber is currently located. The LAI and the TMSI are maintained in both the Mobile Station and the Location Registers (see below).

11. Home Location Register (HLR)

Register where the references to the subscriber having subscribed locally are maintained. The HLR is in fact a (piece of a) data base in a specialized computer.

12. Visitor Location Register (VLR)

Register where the references to "roaming" subscribers considered currently as visitors are maintained. The VLR is in fact a (piece of a) data base in a specialized computer.

13. Key for Authentication (Ki)

The Subscriber Authentication key Ki is a fixed, secret and personal key which is used to authenticate the subscriber upon accessing the network. Ki is used to compute the Signed Response (see below) and the Cipherring Key (see below)

14. Key for Cipherring (Kc)

The Cipherring Key Kc is used to cipher/decipher the data transmitted over the RF channel, thus providing confidentiality of the transmission. Kc is only valid for one session, i.e. from one authentication until the next one.

15. Signed Response (SRES)

The Signed Response is a signature number computed by the authentication algorithm A3 (see below), using a random number and the key Ki as inputs. The SRES is computed in the SIM of the Mobile Station, and sent back to the originator of the random number for comparison with a value computed locally.

16. Algorithm A3

A3 is the name of the algorithm used to authenticate the subscriber. A3 uses a random number and Ki as inputs, and produces SRES.

17. Algorithm A5

A5 is the name of the algorithm used to cipher/decipher the transmission data. A5 is computed using Kc at both ends of the transmission, with one end being the Mobile Equipment.

18. Algorithm A8

A8 is the name of the algorithm used to compute Kc. A8 is coupled to A3 and uses a random number and Ki as inputs.

19. Personal Identification Code (PIN)

A four digit number which can be used by the subscriber to prevent unauthorized usage of his Mobile Station. The PIN code may be changed by the user.

20. Data-Field

A logical data area within the SIM, which contains information having the same security access conditions and data management characteristics.

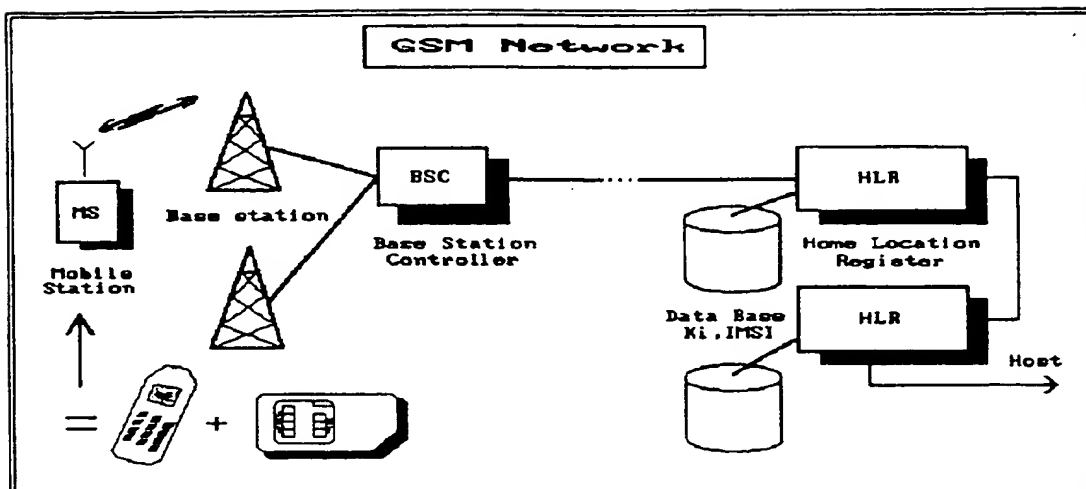
A data-field may be either "binary" (non-structured data-field composed of a fixed length block), or "formatted" (organized in logical records of fixed length).

21. Directory

Data-fields are grouped logically into directories.

B. Architecture

A diagram showing the simplified architecture of the GSM system is shown hereafter:



C. Services

Potential services offered to the subscribers include:

- Telephone calls (voice): make and receive
 - Emergency calls
 - Transmission of short alphanumeric messages
 - Group 3 facsimile transmission
 - Connection to packet-switched networks such as X25
- Additional features can be:

- Abbreviated dialing numbers
- Fixed dialing numbers
- Collecting charging information
- Barring of outgoing calls

It should be noted that a subscriber is always identified in the same way, whatever his geographical location at any point in time. This means that a "fixed" number can be used to reach a travelling person. This opens the doors to much more efficient business telecommunications.

Also, thanks to the basic bit-rate of 270.83 Kb/s, many tele-informatics applications will be possible.

IV. THE SIM FUNCTIONS

A. General features

As mentioned above, the SIM is the part of the Mobile Station which contains the information related to the subscriber's identity and his specific data.

But the SIM is not just a passive device: it participates actively in the security of the system by executing part of the algorithmic processes. The SIM actively authenticates itself, checks the identity of the user, and initializes the encryption of the transmission link. Therefore, the SIM has two fundamental purposes:

- storing data (and controlling the access to this data)
- executing algorithms in secure conditions

Because it is removable, the remainder of the Mobile Station, i.e. the Mobile Equipment, is generic and not user-dependent; in particular, a ME is not associated to a defined call number. This gives a greater flexibility for the Operators to manage their base of stations and subscribers. In fact, all the Operators have to manage is the SIMs themselves, not the stations. The commercial relationship between the Operator and the Subscriber translates into the Subscriber being allocated a SIM.

The SIM concept allows the manufacturers of Mobile Equipments to be independent from the way the Operators may handle their system, and thus manufacture generic, standardized devices with no access-control functions.

Thanks to its small size and removability, the SIM can be carried around by its user in a wallet, to be plugged in different stations and different locations, as the needs arise.

What the SIM does not do, is decide which services are accessible to the user and which are not. The choice has been made to not store entitlements or rights inside the SIM, but rather have a centralized access-control management. Which services are accessible to a particular user, is decided and checked by the central system, after having carried out the authentication of the SIM through the ME and the network.

B. Storage functions

The SIM is in charge of storing some of the essential information needed to operate the system. Also, an Operator may choose to store in the SIM some optional data needed to implement additional features.

1. Basic storage functions

The Subscriber is identified uniquely in the set of GSM PLMNs by its International Mobile Subscriber Identity number. This number needs to be stored securely within the SIM so that the Subscriber can be recognized unambiguously at whatever station he may use. The IMSI is a fixed number.

A Mobile Station can only be operated if there is a valid IMSI in the SIM, except for emergency calls.

Next to the IMSI, the SIM stores the TMSI (Temporary Mobile Subscriber Identity), which is the code most often used to address the Subscriber: the TMSI is only valid locally, and for a short period of time. It is used in place of the IMSI so as to maintain the identity of the Subscriber confidential.

In order to preserve the correspondence between the IMSI and the TMSI, the Location Area Identity number is needed. Like the TMSI, the LAI is not a fixed piece of data and may be replaced when re-localizing a customer.

Associated to the IMSI, is the Key for Authentication K_i , which is used as an input to the authentication algorithm. K_i is fixed and stored in a secure location.

The SIM also stores temporarily the Key for Ciphering K_c , after having computed it with the A3 algorithm (see paragraph Security functions), and before passing it to the ME. Cipher Keys are indexed with a sequence number, which is also stored in the SIM.

The SIM stores the current value of the PIN code, which it is responsible for checking (see paragraph security functions)

The SIM stores the time value related to the periodic location updating. This value is called TMSI time.

In addition, the SIM must maintain some data associated with the "house-keeping" functions such as:

- PIN error counter
- personal unblocking key
- any secret code related to administration procedures

2. Optional storage functions

The SIM may provide facilities to store and manage additional information related to the mobile subscriber in association with the GSM services:

a) Directory of abbreviated dialing numbers:

The Subscriber may store in the SIM several telephone numbers associated with a mnemonic alphanumeric identifier. This creates a directory of quick-dial numbers which can be entered via the keyboard of the ME for later use. The size of this directory is determined at the SIM personalization stage.

The memory organization in the SIM for this data is such that these dialing numbers can be shared with another application residing in the (same) SIM.

b) Short message storage:

Short alphanumeric messages can be sent to the GSM Subscriber and stored inside his SIM. Those messages being stored in non volatile memory, they can be retrieved later on, either using the same or a different Mobile Equipment.

C. Security functions

Beside storing essential GSM information, and controlling access to the sensitive data such as IMSI and Ki, the SIM participates actively in the security of the whole system:

1. Authentication of the user to the SIM

In order to prevent unauthorized use of a Mobile Station, when left unattended or when stolen, the SIM provides a PIN code function.

The user is asked to enter a PIN code via the keyboard of the ME in order to identify himself.

The PIN code is a four-digit decimal number which is checked locally by the SIM. If the code presented corresponds with the one inside the SIM, then the authentication is successful; in case of false presentation, the SIM increments securely an error counter. After the counter has detected three false consecutive presentations, the SIM blocks itself.

Once blocked, the SIM is no longer usable for GSM operation. The SIM may be unblocked through the use of a personal Unblocking Key. An unblocking error counter is used to restrict the SIM to a maximum of 10 unsuccessful unblocking procedures.

The SIM comes with a pre-programmed PIN code which the user is free to change as he wishes.

The Operator may offer the possibility for the Subscriber to disable the PIN code function of the SIM. When this capability is not offered, then the user is forced to always enter his PIN code when using a MS with his SIM.

2. Authentication of the SIM to the Network

The GSM network needs to make sure that a MS requesting services corresponds to a genuine Subscriber, before that Subscriber is given access to those services and is charged for them.

The network sends a random challenge RAND, in the form of a 128 bit number, to the SIM. The SIM executes algorithm A3 internally, using RAND and Ki as inputs, and produces SRES. This signature is checked by the network with a similar algorithm; if the signature is recognized as valid, then the authentication is successful.

3. Ciphering of the transmission data

The SIM is not responsible for executing the Ciphering Algorithm A5, which resides in the ME; however, it is responsible for the computation of the Kc key used by A5.

In parallel with A3, the SIM contains the algorithm A8, which uses RAND and Ki as inputs, and produces Kc. Kc is also computed by the fixed part of the network, and is then used for the ciphering/deciphering of the following data transmissions.

V. THE SIM IMPLEMENTATION

Because of the requirements assessed above that the SIM should:

- be detachable
- provide secure storage
- execute algorithms
- be updatable
- exist in two form-factors

the SIM implementation is based on advanced Smart Card technology involving several enhanced features in the field of:

- memory and chip technology
- physical layout and characteristics
- logical memory organization and management

A. Memory and component technology

Because the SIM maintains a great deal of updatable data such as the TMSI, the LAI, Kc, abbreviated phone numbers, or charging information, it is necessary to use erasable memory such as EEPROM which can be erased and re-written tens of thousands of times.

1. component

The GEMPLUS implementation of the SIM uses a CMOS mono-chip component with microprocessor, ROM, RAM and EEPROM memory on the same die. The capabilities of the EEPROM memory have been further enhanced, in terms of number of erase/re-write cycles, by a special procedure which detects weakening memory cells and compensates for the weakening as far as possible.

2. low-power mode

Furthermore, the component used for the SIM provides a "Wait" mode where the CLK signal to the chip can be halted to reduce the power consumption. Such a low-power mode is particularly needed in portable and hand-held models where battery life is critical.

B. Physical layout

The GSM has retained two physical implementations of the SIM:

1. Card SIM

The SIM can be in the form of an ISO-standard card, conforming to the rules of IS7816-1, -2, and -3. The Card SIM is inserted in the ME whenever the Subscriber wants to use it, and is removed when the MS is unattended.

2. Plug-In SIM

The SIM may be a small dedicated module, called "Plug-In Module", mainly intended to be used in portable and hand-held stations where small dimensions are essential. In this case, the physical layout of the SIM must conform to the GSM specifications, while the electrical and logical interface is still ruled by IS7816-3. The Plug-In SIM is obtained by cutting away excessive plastic of the Card SIM, and adding a feature for orientation.

Because a Plug-In SIM is significantly smaller than a credit card, it is not as handy and is intended to be semi-permanently installed in the station. It is up to the manufacturers of MEs to make it more or less easy to install and remove a Plug-In SIM.

Thanks to its unique manufacturing techniques based on molding, GEMPLUS is able to manufacture both Card SIMs and Plug-In SIMs very cost-efficiently.

C. SIM-ME communication protocols

As usual, two levels are distinguished to describe the communication protocol:

- the transmission protocol
- the application protocol

1. Transmission protocol

Regardless of whether the SIM is a Card or a Plug-In module, the transmission protocol conforms to the ISO IS7816-3 standard, using the character mode "T=0".

Although some newer protocols are currently under discussion in the ISO, it was necessary to agree on existing standards in order to match the 1991 deadline. The transmission protocol chosen is quite well adapted to the SIM application.

2. Application protocol

Messages exchanged between the SIM and the ME (or between the SIM and an accepting device during the administrative phase) are divided into:

- Commands (sent to the SIM)
- Responses (received from the SIM)

A GSM instruction is made up of a Command-Response pair, where a response is associated to one command. The response contains condition codes that may be accompanied by data.

A GSM procedure is a sequence of instructions which is supposed to be executed without interruption. Examples of procedures can be:

- User PIN code verification
- IMSI request
- short message erasure

D. SIM memory organization and management

1. Directories and data-fields

Information stored in the SIM is organized in Data-Fields, grouped by Directories.

All information inside a data-field is of the same level of security management.

2. Structure of the directories

Data-fields are grouped in directories related to a specific application or service.

Application Directories (AD) are under the Root Directory (RD).

For the GSM application, there are two Application Directories:

- the GSM directory which contains the GSM
- specific information such as IMSI, LAI
- the Telecom directory which contains the optional information such as abbreviated numbers or charging information. The data in the Telecom Directory may be shared with other applications.

3. Structure of the data-fields

There are two types of data-fields:

- binary data-fields, organized in bytes
 - formatted data-fields, organized in logical records,
- where a logical record is a group of consecutive bytes with a fixed length
- Binary data fields are addressed by block number, offset in the block and length of string in bytes.

Formatted data-fields offer a more flexible addressing method, where a record may be addressed by:

- its absolute number
- a pointer
- seeking a pattern

4. Actions on data-fields and directories

Actions that can be performed on data-fields, when in GSM mode include:

- selection
- update the contents
- read the contents
- seek (in the case of formatted data-fields)

The only action allowed on Directories in GSM mode is:

E. Security Policies

The definition of the rules allowing a specific party to access and perform specific actions on data stored in the SIM is called a security policy.

A security policy is attached to each data-field, which is the smallest entity which can be protected by an individual policy. The various actions that can be performed on a data-field must meet the access conditions specified in the security policy of the target data-field.

Also, a security policy of a higher level may be attached to the Directories. When this is the case, then both the security policy of the directory and the security policy of the data-fields belonging to that directory must be respected in order to perform any action.

The security policy for directories and for the data-fields have the same structure and include conditions for six actions:

- Read or Seek
- Update

Each condition is handled independently and can take the following values:

- ALWays possible (no checking)
- PIN: allowed if PIN code checked or PIN function disabled
- ADM: allowed if an authentication procedure used at the administrative phase has been successful
- NEVer possible

THIS PAGE BLANK (USPTO)

PCTWORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : H04Q 7/38, H04B 7/24		A1	(11) International Publication Number: WO 96/41493
			(43) International Publication Date: 19 December 1996 (19.12.96)
(21) International Application Number: PCT/SE96/00716 (22) International Filing Date: 31 May 1996 (31.05.96) (30) Priority Data: 08/482,754 7 June 1995 (07.06.95) US (71) Applicant: TELEFONAKTIEBOLAGET LM ERICSSON (publ) [SE/SE]; S-126 25 Stockholm (SE). (72) Inventors: DIACHINA, John, W.; 505 Kristin Drive, Garner, NC 27529 (US). RAITH, Alex, K.; Park Ridge Road 805-A5, Durham, NC 27713 (US). PERSSON, Bengt; P.O. Box 42, S-182 05 Djurshamn (SE). SAMMARCO, Anthony, J.; 605 Benfield Court, Garner, NC 27529 (US). (74) Agents: BOHLIN, Björn et al.; Telefonaktiebolaget LM Ericsson, Patent and Trademark Dept., S-126 25 Stockholm (SE).		(81) Designated States: AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG). Published <i>With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i>	
(54) Title: DIGITAL CONTROL CHANNELS HAVING LOGICAL CHANNELS SUPPORTING BROADCAST SMS			
(57) Abstract <p>A communications system in which information is transmitted in successive time slots grouped into a plurality of superframes which are, in turn, grouped into a plurality of hyperframes. A remote station is assigned to one of the time slots in each of the superframes for paging the remote station, each hyperframe including at least two superframes, and the information sent in the assigned time slot in one superframe in each hyperframe is repeated in the assigned time slot in the other superframe(s) in each hyperframe. Each superframe can include a plurality of time slots used for sending paging messages to remote stations, grouped into a plurality of successive paging frames, and the time slot to which the remote station is assigned is included once in every paging frame. Also, each superframe may include time slots comprising a logical channel for broadcast control information and time slots comprising a logical paging channel. Information sent in the assigned time slot may direct the remote station to read the broadcast control information, and the information may have been encoded according to an error correcting code and include a plurality of bits having polarities that are inverses of cyclic redundancy check bits produced by the encoding. Also, the broadcast control information may comprise special messages that are included in respective time slots comprising a logical special message channel, the time slots of the special message channel may be grouped in successive SMS frames, and the SMS frames may be synchronized to start with a start of a superframe.</p>			

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	GB	United Kingdom	MW	Malawi
AT	Austria	GE	Georgia	MX	Mexico
AU	Australia	GN	Guinea	NE	Niger
BB	Barbados	GR	Greece	NL	Netherlands
BE	Belgium	HU	Hungary	NO	Norway
BF	Burkina Faso	IE	Ireland	NZ	New Zealand
BG	Bulgaria	IT	Italy	PL	Poland
BJ	Benin	JP	Japan	PT	Portugal
BR	Brazil	KE	Kenya	RO	Romania
BY	Belarus	KG	Kyrgyzstan	RU	Russian Federation
CA	Canada	KP	Democratic People's Republic of Korea	SD	Sudan
CF	Central African Republic	KR	Republic of Korea	SE	Sweden
CG	Congo	KZ	Kazakhstan	SG	Singapore
CH	Switzerland	LI	Liechtenstein	SI	Slovenia
CI	Côte d'Ivoire	LK	Sri Lanka	SK	Slovakia
CM	Cameroon	LR	Liberia	SN	Senegal
CN	China	LT	Lithuania	SZ	Swaziland
CS	Czechoslovakia	LU	Luxembourg	TD	Chad
CZ	Czech Republic	LV	Latvia	TG	Togo
DE	Germany	MC	Monaco	TJ	Tajikistan
DK	Denmark	MD	Republic of Moldova	TT	Trinidad and Tobago
EE	Estonia	MG	Madagascar	UA	Ukraine
ES	Spain	ML	Mali	UG	Uganda
FI	Finland	MN	Mongolia	US	United States of America
FR	France	MR	Mauritania	UZ	Uzbekistan
GA	Gabon			VN	Viet Nam

-1-

DIGITAL CONTROL CHANNELS HAVING LOGICAL CHANNELS SUPPORTING BROADCAST SMS

This application is a continuation-in-part of U.S. Patent Application No. 08/331,703 entitled "Digital Control Channels Having Logical Channels for
5 Multiple Access Radiocommunication", which was filed on October 31, 1994 and which is incorporated in this application by reference. This parent application is a continuation in part of U.S. Patent Application No. 08/147,254 entitled "A
10 Method for Communicating in a Wireless Communication System", which was filed on November 1, 1993, and which is incorporated in this application by reference. The parent application is also a continuation in part of U.S. Patent Application No. 07/956,640 entitled "Digital Control Channel", which was filed on October 5, 1992, and which is incorporated in this application by reference.

BACKGROUND

Applicants' invention relates generally to radiocommunication systems
15 that use digital control channels in a multiple access scheme and more particularly to cellular TDMA radiotelephone systems having digital control channels.

The growth of commercial radiocommunications and, in particular, the explosive growth of cellular radiotelephone systems have compelled system
20 designers to search for ways to increase system capacity without reducing communication quality beyond consumer tolerance thresholds. One way to increase capacity is to use digital communication and multiple access techniques such as TDMA, in which several users are assigned respective time slots on a single radio carrier frequency.

25 In North America, these features are currently provided by a digital cellular radiotelephone system called the digital advanced mobile phone service (D-AMPS), some of the characteristics of which are specified in the interim standard IS-54B, "Dual-Mode Mobile Station-Base Station Compatibility

-2-

Standard", published by the Electronic Industries Association and Telecommunications Industry Association (EIA/TIA). Because of a large existing consumer base of equipment operating only in the analog domain with frequency-division multiple access (FDMA), IS-54B is a dual-mode (analog and digital) standard, providing for analog compatibility in tandem with digital communication capability. For example, the IS-54B standard provides for both FDMA analog voice channels (AVC) and TDMA digital traffic channels (DTC), and the system operator can dynamically replace one type with the other to accommodate fluctuating traffic patterns among analog and digital users. The AVCs and DTCs are implemented by frequency modulating radio carrier signals, which have frequencies near 800 megahertz (MHz) such that each radio channel has a spectral width of 30 kilohertz (KHz).

In a TDMA cellular radiotelephone system, each radio channel is divided into a series of time slots, each of which contains a burst of information from a data source, e.g., a digitally encoded portion of a voice conversation. The time slots are grouped into successive TDMA frames having a predetermined duration. The number of time slots in each TDMA frame is related to the number of different users that can simultaneously share the radio channel. If each slot in a TDMA frame is assigned to a different user, the duration of a TDMA frame is the minimum amount of time between successive time slots assigned to the same user.

The successive time slots assigned to the same user, which are usually not consecutive time slots on the radio carrier, constitute the user's digital traffic channel, which may be considered a logical channel assigned to the user. As described in more detail below, digital control channels (DCCHs) can also be provided for communicating control signals, and such a DCCH is a logical channel formed by a succession of usually non-consecutive time slots on the radio carrier.

According to IS-54B, each TDMA frame consists of six consecutive time slots and has a duration of 40 milliseconds (msec). Thus, each radio channel can

-3-

carry from three to six DTCs (e.g., three to six telephone conversations), depending on the source rates of the speech coder/decoders (codecs) used to digitally encode the conversations. Such speech codecs can operate at either full-rate or half-rate, with full-rate codecs being expected to be used until half-rate
5 codecs that produce acceptable speech quality are developed. A full-rate DTC requires twice as many time slots in a given time period as a half-rate DTC, and in IS-54B, each radio channel can carry up to three full-rate DTCs or up to six half-rate DTCs. Each full-rate DTC uses two slots of each TDMA frame, i.e., the first and fourth, second and fifth, or third and sixth of a TDMA frame's six
10 slots. Each half-rate DTC uses one time slot of each TDMA frame. During each DTC time slot, 324 bits are transmitted, of which the major portion, 260 bits, is due to the speech output of the codec, including bits due to error correction coding of the speech output, and the remaining bits are used for guard times and overhead signalling for purposes such as synchronization.

15 It can be seen that the TDMA cellular system operates in a buffer-and-burst, or discontinuous-transmission, mode: each mobile station transmits (and receives) only during its assigned time slots. At full rate, for example, a mobile station might transmit during slot 1, receive during slot 2, idle during slot 3, transmit during slot 4, receive during slot 5, and idle during slot 6, and then
20 repeat the cycle during succeeding TDMA frames. Therefore, the mobile station, which may be battery-powered, can be switched off, or sleep, to save power during the time slots when it is neither transmitting nor receiving. In the IS-54B system in which the mobile does not transmit and receive simultaneously, a mobile can sleep for periods of at most about 27 msec (four slots) for a half-
25 rate DTC and about 7 msec (one slot) for a full-rate DTC.

In addition to voice or traffic channels, cellular radiocommunication systems also provide paging/access, or control, channels for carrying call-setup messages between base stations and mobile stations. According to IS-54B, for example, there are twenty-one dedicated analog control channels (ACCs), which
30 have predetermined fixed frequencies for transmission and reception located near

800 MHz. Since these ACCs are always found at the same frequencies, they can be readily located and monitored by the mobile stations.

For example, when in an idle state (i.e., switched on but not making or receiving a call), a mobile station in an IS-54B system tunes to and then
5 regularly monitors the strongest control channel (generally, the control channel of the cell in which the mobile station is located at that moment) and may receive or initiate a call through the corresponding base station. When moving between
10 cells while in the idle state, the mobile station will eventually "lose" radio connection on the control channel of the "old" cell and tune to the control channel of the "new" cell. The initial tuning and subsequent re-tuning to control channels are both accomplished automatically by scanning all the available control channels at their known frequencies to find the "best" control channel. When a control channel with good reception quality is found, the mobile station remains tuned to this channel until the quality deteriorates again. In this way,
15 mobile stations stay "in touch" with the system. The ACCs specified in IS-54B require the mobile stations to remain continuously "awake" (or at least for a significant part of the time, e.g. 50%) in the idle state, at least to the extent that they must keep their receivers switched on.

While in the idle state, a mobile station must monitor the control channel
20 for paging messages addressed to it. For example, when an ordinary telephone (land-line) subscriber calls a mobile subscriber, the call is directed from the public switched telephone network (PSTN) to a mobile switching center (MSC) that analyzes the dialed number. If the dialed number is validated, the MSC requests some or all of a number of radio base stations to page the called mobile
25 station by transmitting over their respective control channels paging messages that contain the mobile identification number (MIN) of the called mobile station. Each idle mobile station receiving a paging message compares the received MIN with its own stored MIN. The mobile station with the matching stored MIN transmits a page response over the particular control channel to the base station,
30 which forwards the page response to the MSC.

-5-

Upon receiving the page response, the MSC selects an AVC or a DTC available to the base station that received the page response, switches on a corresponding radio transceiver in that base station, and causes that base station to send a message via the control channel to the called mobile station that
5 instructs the called mobile station to tune to the selected voice or traffic channel. A through-connection for the call is established once the mobile station has tuned to the selected AVC or DTC.

When a mobile subscriber initiates a call, e.g., by dialing the telephone number of an ordinary subscriber and pressing the "send" button on the mobile
10 station, the mobile station transmits the dialed number and its MIN and an electronic serial number (ESN) over the control channel to the base station. The ESN is a factory-set, "unchangeable" number designed to protect against the unauthorized use of the mobile station. The base station forwards the received numbers to the MSC, which validates the mobile station, selects an AVC or
15 DTC, and establishes a through-connection for the call as described above. The mobile may also be required to send an authentication message.

It will be understood that a communication system that uses ACCs has a number of deficiencies. For example, the format of the forward analog control channel specified in IS-54B is largely inflexible and not conducive to the
20 objectives of modern cellular telephony, including the extension of mobile station battery life. In particular, the time interval between transmission of certain broadcast messages is fixed and the order in which messages are handled is also rigid. Also, mobile stations are required to re-read messages that may not have changed, wasting battery power. These deficiencies can be remedied by
25 providing a DCCH having new formats and processes, one example of which is described in U.S. Patent Application No. 07/956,640 entitled "Digital Control Channel", which was filed on October 5, 1992, and which is incorporated in this application by reference. Using such DCCHs, each IS-54B radio channel can carry DTCs only, DCCHs only, or a mixture of both DTCs and DCCHs.
30 Within the IS-54B framework, each radio carrier frequency can have up to three

-6-

full-rate DTCs/DCCHs, or six half-rate DTCs/DCCHs, or any combination in-between, for example, one full-rate and four half-rate DTCs/DCCHs. As described in this application, a DCCH in accordance with Applicants' invention provides a further increase in functionality.

5 In general, however, the transmission rate of the DCCH need not coincide with the half-rate and full-rate specified in IS-54B, and the length of the DCCH slots may not be uniform and may not coincide with the length of the DTC slots. The DCCH may be defined on an IS-54B radio channel and may consist, for example, of every n-th slot in the stream of consecutive TDMA slots. In this
10 case, the length of each DCCH slot may or may not be equal to 6.67 msec, which is the length of a DTC slot according to IS-54B. Alternatively (and without limitation on other possible alternatives), these DCCH slots may be defined in other ways known to one skilled in the art.

 As such hybrid analog/digital systems mature, the number of analog users
15 should diminish and the number of digital users should increase until all of the analog voice and control channels are replaced by digital traffic and control channels. When that occurs, the current dual-mode mobile terminals can be replaced by less expensive digital-only mobile units, which would be unable to scan the ACCs currently provided in the IS-54B system. One conventional
20 radiocommunication system used in Europe, known as GSM, is already an all-digital system, in which 200-KHz-wide radio channels are located near 900 MHz. Each GSM radio channel has a gross data rate of 270 kilobits per second and is divided into eight full-rate traffic channels (each traffic time slot carrying 116 encrypted bits).

25 In cellular telephone systems, an air-interface communications link protocol is required in order to allow a mobile station to communicate with the base stations and MSC. The communications link protocol is used to initiate and to receive cellular telephone calls. As described in U.S. Patent Application No. 08/047,452 entitled "Layer 2 Protocol for the Random Access Channel and
30 the Access Response Channel," which was filed on April 19, 1993, and which is

-7-

incorporated in this application by reference, the communications link protocol is commonly referred to within the communications industry as a Layer 2 protocol, and its functionality includes the delimiting, or framing, of Layer 3 messages. These Layer 3 messages may be sent between communicating Layer 3 peer entities residing within mobile stations and cellular switching systems. The physical layer (Layer 1) defines the parameters of the physical communications channel, e.g., radio frequency spacing, modulation characteristics, etc. Layer 2 defines the techniques necessary for the accurate transmission of information within the constraints of the physical channel, e.g., error correction and detection, etc. Layer 3 defines the procedures for reception and processing of information transmitted over the physical channel.

Communications between mobile stations and the cellular switching system (the base stations and the MSC) can be described in general with reference to FIGS. 1 and 2. FIG. 1 schematically illustrates pluralities of Layer 3 messages 11, Layer 2 frames 13, and Layer 1 channel bursts, or time slots, 15. In FIG. 1, each group of channel bursts corresponding to each Layer 3 message may constitute a logical channel, and as described above, the channel bursts for a given Layer 3 message would usually not be consecutive slots on an IS-54B carrier. On the other hand, the channel bursts could be consecutive; as soon as one time slot ends, the next time slot could begin.

Each Layer 1 channel burst 15 contains a complete Layer 2 frame as well as other information such as, for example, error correction information and other overhead information used for Layer 1 operation. Each Layer 2 frame contains at least a portion of a Layer 3 message as well as overhead information used for Layer 2 operation. Although not indicated in FIG. 1, each Layer 3 message would include various information elements that can be considered the payload of the message, a header portion for identifying the respective message's type, and possibly padding.

Each Layer 1 burst and each Layer 2 frame is divided into a plurality of different fields. In particular, a limited-length DATA field in each Layer 2

-8-

frame contains the Layer 3 message 11. Since Layer 3 messages have variable lengths depending upon the amount of information contained in the Layer 3 message, a plurality of Layer 2 frames may be needed for transmission of a single Layer 3 message. As a result, a plurality of Layer 1 channel bursts may also be needed to transmit the entire Layer 3 message as there is a one-to-one correspondence between channel bursts and Layer 2 frames.

As noted above, when more than one channel burst is required to send a Layer 3 message, the several bursts are not usually consecutive bursts on the radio channel. Moreover, the several bursts are not even usually successive bursts devoted to the particular logical channel used for carrying the Layer 3 message. Since time is required to receive, process, and react to each received burst, the bursts required for transmission of a Layer 3 message are usually sent in a staggered format, as schematically illustrated in FIG. 2 and as described above in connection with the IS-54B standard.

FIG. 2 shows a general example of a forward (or downlink) DCCH configured as a succession of time slots 1, 2, . . . , N, . . . included in the consecutive time slots 1, 2, . . . sent on a carrier frequency. These DCCH slots may be defined on a radio channel such as that specified by IS-54B, and may consist, as seen in FIG. 2 for example, of every n-th slot in a series of consecutive slots. Each DCCH slot has a duration that may or may not be 6.67 msec, which is the length of a DTC slot according to the IS-54B standard.

As shown in FIG. 2, the DCCH slots may be organized into superframes (SF), and each superframe includes a number of logical channels that carry different kinds of information. One or more DCCH slots may be allocated to each logical channel in the superframe. The exemplary downlink superframe in FIG. 2 includes three logical channels: a broadcast control channel (BCCH) including six successive slots for overhead messages; a paging channel (PCH) including one slot for paging messages; and an access response channel (ARCH) including one slot for channel assignment and other messages. The remaining time slots in the exemplary superframe of FIG. 2 may be dedicated to other

logical channels, such as additional paging channels PCH or other channels. Since the number of mobile stations is usually much greater than the number of slots in the superframe, each paging slot is used for paging several mobile stations that share some unique characteristic, e.g., the last digit of the MIN.

5 For purposes of efficient sleep mode operation and fast cell selection, the BCCH may be divided into a number of sub-channels. U.S. Patent Application No. 07/956,640 discloses a BCCH structure that allows the mobile station to read a minimum amount of information when it is switched on (when it locks onto a DCCH) before being able to access the system (place or receive a call). After
10 being switched on, an idle mobile station needs to regularly monitor only its assigned PCH slots (usually one in each superframe); the mobile can sleep during other slots. The ratio of the mobile's time spent reading paging messages and its time spent asleep is controllable and represents a tradeoff between call-set-up delay and power consumption.

15 Since each TDMA time slot has a certain fixed information carrying capacity, each burst typically carries only a portion of a Layer 3 message as noted above. In the uplink direction, multiple mobile stations attempt to communicate with the system on a contention basis, while multiple mobile stations listen for Layer 3 messages sent from the system in the downlink
20 direction. In known systems, any given Layer 3 message must be carried using as many TDMA channel bursts as required to send the entire Layer 3 message.

Digital control and traffic channels are desirable for these and other reasons described in U.S. Patent Application No. 08/147,254, entitled "A Method for Communicating in a Wireless Communication System", which was
25 filed on November 1, 1993, and which is incorporated in this application by reference. For example, they support longer sleep periods for the mobile units, which results in longer battery life. Although IS-54B provides for digital traffic channels, more flexibility is desirable in using digital control channels having expanded functionality to optimize system capacity and to support hierarchical
30 cell structures, i.e., structures of macrocells, microcells, picocells, etc. The

-10-

term "macrocell" generally refers to a cell having a size comparable to the sizes of cells in a conventional cellular telephone system (e.g., a radius of at least about 1 kilometer), and the terms "microcell" and "picocell" generally refer to progressively smaller cells. For example, a microcell might cover a public indoor or outdoor area, e.g., a convention center or a busy street, and a picocell might cover an office corridor or a floor of a high-rise building. From a radio coverage perspective, macrocells, microcells, and picocells may be distinct from one another or may overlap one another to handle different traffic patterns or radio environments.

FIG. 3 is an exemplary hierarchical, or multi-layered, cellular system. An umbrella macrocell 10 represented by a hexagonal shape makes up an overlying cellular structure. Each umbrella cell may contain an underlying microcell structure. The umbrella cell 10 includes microcell 20 represented by the area enclosed within the dotted line and microcell 30 represented by the area enclosed within the dashed line corresponding to areas along city streets, and picocells 40, 50, and 60, which cover individual floors of a building. The intersection of the two city streets covered by the microcells 20 and 30 may be an area of dense traffic concentration, and thus might represent a hot spot.

FIG. 4 represents a block diagram of an exemplary cellular mobile radiotelephone system, including an exemplary base station 110 and mobile station 120. The base station includes a control and processing unit 130 which is connected to the MSC 140 which in turn is connected to the PSTN (not shown). General aspects of such cellular radiotelephone systems are known in the art, as described by the above-cited U.S. patent applications and by U.S. Patent No. 5,175,867 to Wejke et al., entitled "Neighbor-Assisted Handoff in a Cellular Communication System," and U.S. Patent Application No. 07/967,027 entitled "Multi-mode Signal Processing," which was filed on October 27, 1992, both of which are incorporated in this application by reference.

The base station 110 handles a plurality of voice channels through a voice channel transceiver 150, which is controlled by the control and processing

-11-

unit 130. Also, each base station includes a control channel transceiver 160, which may be capable of handling more than one control channel. The control channel transceiver 160 is controlled by the control and processing unit 130. The control channel transceiver 160 broadcasts control information over the control channel of the base station or cell to mobiles locked to that control channel. It will be understood that the transceivers 150 and 160 can be implemented as a single device, like the voice and control transceiver 170, for use with DCCHs and DTCs that share the same radio carrier frequency.

The mobile station 120 receives the information broadcast on a control channel at its voice and control channel transceiver 170. Then, the processing unit 180 evaluates the received control channel information, which includes the characteristics of cells that are candidates for the mobile station to lock on to, and determines on which cell the mobile should lock. Advantageously, the received control channel information not only includes absolute information concerning the cell with which it is associated, but also contains relative information concerning other cells proximate to the cell with which the control channel is associated, as described in U.S. Patent No. 5,353,332 to Raith et al., entitled "Method and Apparatus for Communication Control in a Radiotelephone System," which is incorporated in this application by reference.

As noted above, one of the goals of a digital cellular system is to increase the user's "talk time", i.e., the battery life of the mobile station. To this end, U.S. Patent Application No. 07/956,640 discloses a digital forward control channel (base station to mobile station) that can carry the types of messages specified for current analog forward control channels (FOCCs), but in a format which allows an idle mobile station to read overhead messages when locking onto the FOCC and thereafter only when the information has changed; the mobile sleeps at all other times. In such a system, some types of messages are broadcast by the base stations more frequently than other types, and mobile stations need not read every message broadcast.

-12-

Also, Application No. 07/956,640 shows how a DCCH may be defined alongside the DTCs specified in IS-54B. For example, a half-rate DCCH could occupy one slot and a full-rate DCCH could occupy two slots out of the six slots in each TDMA frame. For additional DCCH capacity, additional half-rate or full-rate DCCHs could replace DTCs. In general, the transmission rate of a DCCH need not coincide with the half-rate and full-rate specified in IS-54B, and the length of the DCCH time slots need not be uniform and need not coincide with the length of the DTC time slots.

Although the above-described communication systems are highly beneficial and are markedly different from previous systems, Applicants' communication system is capable of broadcasting special messages to the mobile stations without affecting other aspects of its performance.

SUMMARY

According to an exemplary embodiment of the present invention, broadcast SMS systems can be provided wherein a plurality of messages are transmitted over one or more sub-channels of a logical S-BCCH channel that have a fixed, time multiplexed format relative to other logical channels. Message attributes are specified on a per message basis so that a mobile station will look at the attributes of each message to determine whether or not that message should be read by that mobile station. In this exemplary embodiment, new sub-channels are added by the system as needed to support the number of messages to be transmitted at any given time.

According to another exemplary embodiment of the present invention, broadcast SMS systems can be provided wherein the sub-channel ordering is more flexible since it is not provided in a fixed, time multiplexed format. Message attributes are associated on a sub-channel basis rather than a per message basis. In this way, messages can be grouped into categories based upon subsets of different message attributes and transmitted based upon their grouping.

-13-

Similarly, mobile messages associated with those groups whose attribute(s) match those associated with a subscriber.

BRIEF DESCRIPTION OF THE DRAWINGS

The features and advantages of Applicants' invention will be understood
5 by reading this description in conjunction with the drawings, in which:

FIG. 1 illustrates a plurality of Layer 3 messages, Layer 2 frames, and Layer 1 channel bursts in a communication system;

FIG. 2 is a generalized view of a digital control channel (DCCH) having time slots which are grouped into superframes;

10 FIG. 3 illustrates a typical multi-layered cellular system employing umbrella macrocells, microcells and picocells;

FIG. 4 represents an exemplary implementation of an apparatus for a radiotelephone system according to the present invention;

FIG. 5 shows a hyperframe structure;

15 FIG. 6 shows the logical channels of the DCCH;

FIG. 7 shows an exemplary TDMA frame structure;

FIGS. 8a-8c show exemplary slot formats on the DCCH;

FIG. 9 shows the partitioning of data before channel encoding;

FIG. 10 shows a paging frame structure;

20 FIG. 11 shows an SMS frame structure;

FIG. 12 shows an example of SMS sub-channel multiplexing; and

FIGS. 13a-13c show S-BCCH Layer 2 frames according to a first exemplary broadcast SMS embodiment; and

25 FIGS. 14a-14d show S-BCCH Layer 2 frames according to a second exemplary embodiment.

DETAILED DESCRIPTION

The following description is in terms of a cellular radiotelephone system, but it will be understood that Applicants' invention is not limited to that

-14-

environment. Also, the following description is in the context of TDMA cellular communication systems, but it will be understood by those skilled in the art that the present invention may apply to other digital communication applications such as Code Division Multiple Access (CDMA). The physical channel may be, for example, a relatively narrow band of radio frequencies (FDMA), a time slot on a radio frequency (TDMA), a code sequence (CDMA), or a combination of the foregoing, which can carry speech and/or data, and is not limited to any particular mode of operation, access technique, or system architecture.

In one aspect of Applicants' invention, communication between mobile stations and base stations is structured into successions of different kinds of logical frames. FIG. 5 illustrates the frame structure of a forward (base station to mobile station) DCCH and shows two successive hyperframes (HF), each of which preferably comprises a respective primary superframe (SF) and a respective secondary superframe. It will be recognized, of course, that a hyperframe could include more than two superframes.

Three successive superframes are illustrated in FIG. 5, each comprising a plurality of time slots that are organized as logical channels F-BCCH, E-BCCH, S-BCCH, and SPACH that are described in more detail below. At this point, it is sufficient to note that each superframe in a forward DCCH includes a complete set of F-BCCH information (i.e., a set of Layer 3 messages), using as many slots as are necessary, and that each superframe begins with a F-BCCH slot. After the F-BCCH slot or slots, the remaining slots in each superframe include one or more (or no) slots for the E-BCCH, S-BCCH, and SPACH logical channels.

Referring to FIG. 5, and more particularly to FIG. 6, each superframe of the downlink (forward) DCCH preferably comprises a broadcast control channel BCCH, and a short-message-service/paging/access channel SPACH. The BCCH comprises a fast BCCH (the F-BCCH shown in FIG. 5); an extended BCCH (the E-BCCH); and a short-message-service BCCH (the S-BCCH), all of which are used, in general, to carry generic, system-related information from the base

-15-

stations to the mobiles. The BCCH is unidirectional, shared, point-to-multipoint, and unacknowledged. The SPACH comprises a short-message-service channel SMSCH, a plurality of paging channels PCH, and an access response channel ARCH, which are used to send information to specific mobile stations relating to short-message-service point-to-point messages (SMSCH), paging messages (PCH), and messages responding to attempted accesses (ARCH) as described below. The SPACH is unidirectional, shared, and unacknowledged. The PCH may be considered point-to-multipoint, in that it can be used to send paging messages to more than one mobile station, but in some circumstances the PCH is point-to-point. The ARCH and SMSCH are generally point-to-point, although messages sent on the ARCH can also be addressed to more than one mobile station.

For communication from the mobile stations to the base stations, the reverse (uplink) DCCH comprises a random access channel RACH, which is used by the mobiles to request access to the system. The RACH logical channel is unidirectional, shared, point-to-point, and acknowledged. All time slots on the uplink are used for mobile access requests, either on a contention basis or on a reserved basis. Reserved-basis access is described in U.S. Patent Application No. 08/140,467, entitled "Method of Effecting Random Access in a Mobile Radio System", which was filed on October 25, 1993, and which is incorporated in this application by reference. One important feature of RACH operation is that reception of some downlink information is required, whereby mobile stations receive real-time feedback for every burst they send on the uplink. This is known as Layer 2 ARQ, or automatic repeat request, on the RACH. The downlink information preferably comprises twenty-two bits that may be thought of as another downlink sub-channel dedicated to carrying, in the downlink, Layer 2 information specific to the uplink. This flow of information, which can be called shared channel feedback, enhances the throughput capacity of the RACH so that a mobile station can quickly determine whether any burst of any

-16-

access attempt has been successfully received. Other aspects of the RACH are described below.

5 The F-BCCH logical channel carries time-critical system information, such as the structure of the DCCH, other parameters that are essential for accessing the system, and an E-BCCH change flag that is described in more detail below; as noted above, a complete set of F-BCCH information is sent in every superframe. The E-BCCH logical channel carries system information that is less time-critical than the information sent on the F-BCCH; a complete set of E-BCCH information (i.e., a set of Layer 3 messages) may span several
10 superframes and need not be aligned to start in the first E-BCCH slot of a superframe. The S-BCCH logical channel carries short broadcast messages, such as advertisements and information of interest to various classes of mobile subscriber, and possibly system operation information, such as change flags for the other logical channels. An important aspect of Applicants' invention is that
15 the S-BCCH decouples the system overhead information sent on the F-BCCH and E-BCCH from the broadcast message service (S-BCCH), obtaining maximum system flexibility. It would be possible to omit the S-BCCH and send its messages on the E-BCCH or even the F-BCCH, but doing so would delay the delivery of important system information since the SMS messages would be
20 intermingled with the system overhead messages.

As for the SPACH slots, they are assigned dynamically to the SMSCH, PCH, and ARCH channels based on transmitted header information. The SMSCH logical channel is used to deliver short messages to a specific mobile station receiving SMS services. The PCH logical channel carries paging
25 messages and other orders to the mobiles, such as the F-BCCH change flag described above and in U.S. Patent Application No. 07/956,640. Mobile stations are assigned respective PCH slots in a manner described in more detail below. A mobile station listens to system responses sent on the ARCH logical channel upon successful completion of the mobile's access on a RACH. The ARCH may

-17-

be used to convey AVC or DTC assignments or other responses to the mobile's attempted access.

An important aspect of exemplary embodiments is that every PCH slot in the primary superframe of a hyperframe is repeated in the secondary superframe of that hyperframe. This is called "specification guaranteed repeat". Thus, once a mobile station has read the BCCH information, it can enter sleep mode after determining, based on its MIN or some other distinguishing characteristic, which single PCH slot it is to monitor for a paging message. Then, if the mobile station properly receives a paging message sent in its PCH slot in a primary superframe, the mobile can sleep through the entire associated secondary superframe, thereby increasing the life of its batteries. If and only if the mobile station cannot correctly decode its assigned PCH slot in a primary superframe, the mobile reads the corresponding PCH slot in the associated secondary superframe.

It should be understood, however, that the mobile station may read its PCH slot in only one of the superframes, either primary or secondary, for a variety of reasons, whether or not the slot is correctly decoded. This may be permitted to maximize the mobile's sleep time. Also, after the mobile has read its PCH slot in one of the superframes (for example, a primary superframe), the mobile may monitor other control channels during at least part of the time until the next (primary) superframe without missing a page on the first control channel. Indeed, the mobile may even read a paging slot on another control channel. This enables cell reselection to be carried out smoothly and avoids the mobile's being blind to pages during such reselection. It will be recognized that reselection is facilitated when the two control channels are synchronized, at least to the extent that a time offset between their superframes is known, which is information that may be provided on the E-BCCH for example.

One aspect of a DCCH as described in U.S. Patent Application No. 07/956,640 is that the F-BCCH slots in successive superframes carry the same information until change flags transmitted in the PCH slots toggle, or

-18-

otherwise change value in a predetermined way. This feature is also provided in the systems and methods described in this application. Also, the E-BCCH and S-BCCH information may span both superframes in a hyperframe, and even several hyperframes, which represents a tradeoff between BCCH bandwidth (i.e., the number of slots needed for sending a complete set of BCCH messages) and the time required for a full cycle of messages sent. The toggling of a change flag in the PCH slot indicates that new data will be found on the F-BCCH sent in the following superframe. In this way, once a mobile station has read the BCCH information on a DCCH, the mobile need awaken only to read its assigned PCH slot; when the change flag in its PCH slot toggles, the mobile learns that it must either awaken or stay awake to re-acquire the F-BCCH, which has changed; if the mobile determines that the change flag has not toggled, it is not necessary for the mobile to read the F-BCCH. This also increases the mobile's sleep time, and battery life.

In a similar way, the F-BCCH slots may include E-BCCH change flags indicating that the system has changed the E-BCCH information. In response to an E-BCCH change flag, the mobile would stay awake to read the E-BCCH slots. It will be understood that the change of the E-BCCH change flag in the F-BCCH slots is "new data" to be found on the F-BCCH that would be indicated by the F-BCCH change flag transmitted in the PCH slots. The mobile station preferably stores the value of the E-BCCH change flag transmitted in the F-BCCH slots before reading the E-BCCH. After the mobile station has acquired the relevant information (which may be dependent on the specific task the mobile is engaged in), the mobile reads the E-BCCH change notification flag again. The process of updating/initiating the E-BCCH message set can be considered successful when the E-BCCH change flag is the same before and after the mobile reads the E-BCCH.

Among the other important features of Applicants' invention, is that information is not interleaved among successive slots, although as described below, information may be interleaved among fields in the same slot. Also as

-19-

described below, the downlink information is advantageously encoded by error correction codes for immunity to channel impairments, for example a convolutional rate-1/2 code. It is desirable not to use "too much" encoding like a convolutional rate-1/4 code, however, because the number of user data bits sent in any given channel burst would be low. Also, such encoding is not needed because the BCCH information is repeated in every superframe and certain transactions can use ARQ. The BCCH and PCH cannot use ARQ, of course, but using a single type of coding is advantageous because it reduces equipment complexity. Therefore, to obtain sufficient protection, somewhat less encoding is combined with the time diversity provided by specification guaranteed repeat for the PCH. This combination is also beneficial for sleep mode performance.

The combination of these features results in a communication system that has good immunity to errors at the same time that it permits, on average, long mobile sleep times. It will be appreciated that the guaranteed repeats of the PCH slots provide time diversity, yielding an improved immunity to errors due to Rayleigh fading that is provided in previous systems by rate-1/4 encoding and inter-burst interleaving. (Of course, specification guaranteed repeat is not an option for speech slots.) Applicants' combination of these features, however, results in a communication system that permits a mobile that has successfully decoded its PCH slot in a primary superframe to sleep through all of the PCH slots in the corresponding secondary superframe. It will be recognized that the a mobile's assigned PCH slots are temporally separated by many times the duration of such a slot (6.67 msec).

The BCCH information sent in one or more slots of the DCCH comprises information about the serving system and the desired behavior of the mobile station when operating in this system. The overhead information would include, for example, indications of the following: (1) the paging slot to which the mobile station is assigned; (2) whether the mobile station is allowed to make and receive any calls through this base station or is restricted to only emergency calls; (3) the power level to be used for transmitting to this base station; (4) the

-20-

identity of the system (home system or visited system); (5) whether or not to use an equalizer for compensating distortion and attenuation effects of the radio channel on the transmitted signal; and (6) the location of other DCCHs (frequencies, time slots, time offsets of other DCCHs' superframes with respect to superframes of current DCCH) of neighboring base stations. A DCCH of a neighboring base station may be selected because the DCCH signal received from this base station is too weak or for some other reason, e.g., the signal from another base station is stronger than the signal from this base station.

When a mobile station locks onto the DCCH, the mobile station first reads the overhead information to determine the system identity, call restrictions, etc.; the locations of the DCCHs of the neighboring base stations (the frequencies, time slots, etc., on which these DCCHs may be found); and its paging slot in the superframe (the DCCH slot assigned to the paging frame class to which the mobile station belongs). The relevant DCCH frequencies are stored in memory, and the mobile station then enters sleep mode. Thereafter, the mobile station "awakens" once every hyperframe, depending on the mobile's paging frame class, to read the assigned paging slot, and then returns to sleep.

The F-BCCH information transmitted in every superframe allows a mobile station to read other information in the superframe, to access the system, or to quickly find the best serving cell, when first locking onto a DCCH. For example, certain basic information about the low-layer structure of the DCCH must be read by a mobile station before any other information in the superframe can be read. This basic information includes, for example, a superframe period (number of DCCH slots), whether the DCCH is half-rate or full-rate, the DCCH format (which slot(s) in a TDMA frame), the location of other BCCH channels, the location of the assigned PCH, and whether the mobile station receiver should use an equalizer. Other types of information should also be sent rather often so that a mobile station can quickly accept or reject a particular DCCH. For example, information about the availability and data capability of a cell (the cell may be available only to a closed user group or may not be capable of handling

-21-

data transmissions from a mobile station), the identity of the system and the cell, etc., may be sent in every superframe. For accelerating system accesses, it would be sufficient for a mobile station to read only system access rules sent on the F-BCCH.

- 5 The E-BCCH is assigned a system-controlled, fixed number of slots in each superframe, but a long cycle, or set of messages, sent on the E-BCCH may span several superframes; hence, the number E-BCCH slots in each superframe can be much less than the number of slots needed to carry the long cycle, or set of messages. If there are not enough E-BCCH slots in a superframe to
- 10 accommodate all E-BCCH messages, subsequent superframes are used. Mobile stations are notified through the F-BCCH as described above of the number and location of E-BCCH slots assigned in each superframe. A start-of-E-BCCH marker may be sent in the current F-BCCH (or S-BCCH) to inform the mobile stations that the current superframe contains the start of an E-BCCH message.
- 15 With the E-BCCH, long and/or sporadic information may be sent on the DCCH without affecting the organization of the superframe, e.g., PCH assignments, or the DCCH capacity. For example, the list of DCCHs of neighboring base stations may be sent on the E-BCCH. Such a list can be rather large, including the locations of, say, ten other DCCHs. Such a list would
- 20 require several slots to transmit, and these slots may be spread out over the E-BCCH of several superframes instead of taking up a large portion of one superframe. In this way, BCCH overhead is traded off for a larger number of paging slots (and consequent increased paging capacity).

Layer 1 FORMAT

- 25 An exemplary organization of the information transmitted on each radio channel, i.e., the channel bursts, or time slots, in accordance with Applicants' invention is shown in FIG. 7. This organization is similar to that specified by the IS-54B standard. The consecutive time slots on a radio channel are organized in TDMA frames of six slots each and TDMA blocks of three slots each so that

-22-

a plurality of distinct channels can be supported by a single radio carrier frequency. Each TDMA frame has a duration of 40 msec and supports six half-rate logical channels, three full-rate logical channels, or various combinations between these extremes by interchanging one full-rate channel and two half-rate channels as indicated in the following table. Each slot has a duration of 6.67 msec and carries 324 bits (162 symbols), which have positions in each slot that are conventionally consecutively numbered 1-324.

Number of Slots	Used Slots	Rate
1	1	half
2	1,4	full
4	1,4,2,5	2 full
6	1,4,2,5,3,6	3 full

As explained above, each superframe comprises a predetermined number of successive time slots (full-rate) of a DCCH. Since a complete set of F-BCCH information is sent in each superframe and since the first slot of each superframe is a F-BCCH slot, each superframe is the interval between such initial F-BCCH slots. It is currently preferred that each superframe consist of thirty-two such time slots, which are distributed among the logical channels F-BCCH, E-BCCH, S-BCCH, and SPACH as illustrated in FIG. 5 for example. Thus, the duration of each logical superframe is simply 32 TDMA blocks/superframe * 20 msec/TDMA block = 640 msec, which spans 96 consecutive physical time slots on the radio channel.

It will be appreciated that this selection represents a balance of several factors that Applicants' currently deem most useful. For example, using thirty-two slots, which is an integer power of two, simplifies the implementation of various counters in existing hardware that is based on binary signal processing. Also, using thirty-two-slot superframes balances call set-up delay against paging

-23-

channel (and other channel) capacity. For a given amount of BCCH information to be transmitted, using longer superframes would increase paging capacity, but would also increase the average set-up delay; using shorter superframes would decrease the average set-up delay to an extent, but would also decrease paging capacity and devote a greater proportion of each superframe to overhead information. Different balances can be struck that would nevertheless fall within the spirit of Applicants' invention.

In order to locate each time slot in each superframe and thus provide the enhanced sleep capabilities made available by Applicants' invention, a superframe phase (SFP) count, which increments by one for each full-rate DCCH slot in a given superframe, is included as part of the information broadcast in each downlink DCCH slot. The SFP value sent in the first slot (an F-BCCH slot) of each superframe may be assigned the value 0; the next slot of the same logical DCCH is assigned an SFP value of 1, etc. Thus, for a system using superframes of thirty-two slots each, the SFP value increments modulo-32, and the SFP value sent in each slot requires five bits. For a half-rate DCCH, only half of the values (e.g., 0, 2, 4, . . . , 30) need be used to identify the slots in each superframe of the DCCH.

It will be appreciated that such a modulo-32 up-counter could be replaced by a modulo-32 down-counter, and for a communication system that does not employ superframes having a fixed number of time slots, the modulo-32 up-counter would be replaced by a down counter for indicating the next occurrence of the F-BCCH, or other desired overhead information. It is only necessary for the information in a slot to include some indication of that slot's position in time with respect to the next occurring time slot carrying the important overhead information. It is also desirable that the information indicate the start of the superframe/hyperframe/paging-frame structures, i.e., that the boundaries of the frame structures all be synchronized with the next occurring time slot carrying the important overhead information, but such synchronization is not necessary.

-24-

Two possible formats for the information sent in the slots of the reverse DCCH are shown in FIGS. 8a and 8b, and a preferred information format in the slots of the forward DCCH is shown in FIG. 8c. These formats are substantially the same as the formats used for the DTCs under the IS-54B standard, but new functionalities are accorded to the fields in each slot in accordance with Applicants' invention. In FIGS. 8a-8c, the number of bits in each field is indicated above that field.

In general, messages (Layer 2 user data bits) to be carried by the slots are mapped onto the two DATA fields sent in each slot, and in the downlink slots, encoded SFP values are sent in the CSFP fields that uniquely identify each slot according to each slot's relative position in its superframe. Also in the downlink slots, the BRI, R/N, and CPE fields contain the information used in the random access scheme for Layer 2 ARQ on the RACH; comparable Layer 2 ARQ fields could be included in the uplink slots. In the forward DCCH (FIG. 8c), the DATA fields total 260 bits in length, the CSFP field carries twelve bits, and the BRI, R/N, CPE fields for shared channel feedback total twenty-two bits. In the reverse DCCH, the DATA fields total either a normal 244 bits in length (FIG. 8a) or an abbreviated 200 bits (FIG. 8b).

The bits sent in the G, R, PREAM, SYNC, SYNC+, and AG fields are used in a conventional way to help ensure accurate reception of the CSFP and DATA fields, e.g., for synchronization, guard times, etc. For example, the SYNC field would be the same as that of a DTC according to IS-54B and would carry a predetermined bit pattern used by the base stations to find the start of the slot. Also, the SYNC+ field would include a fixed bit pattern to provide additional synchronization information for the base stations, which would set their receiver gains during the PREAM field so as to avoid signal distortion.

Referring again to FIG. 8c, the CSFP field in each DCCH slot conveys the SFP value that enables the mobile stations to find the start of each superframe. The SFP values are preferably encoded with a (12,8) code, similar to the way the DVCC is encoded according to the IS-54B standard; thus, the

-25-

CSFP field is preferably twelve bits in length, and the unencoded SFP consists of eight bits. Encoding the SFP values in this way has the advantage of using the hardware and software already present in the mobile phone for handling the DVCC. Also, the four check bits are preferably inverted, enabling a mobile to use the information sent in the CSFP field to discriminate between a DCCH and a DTC since the CSFP of a DCCH and the CDVCC of a DTC have no common codewords. Other ways to discriminate DCCHs from DTCs are described in U.S. Patent Application No. 08/147,254. In view of the importance of the SFP to the operation of the system, a mobile station might decode the CSFPs in several slots in order to ensure accuracy since the CSFP in any individual slot is less well protected by encoding and time diversity than the Layer 3 message in the DATA fields.

When each superframe includes thirty-two slots, the three most significant bits in each eight unencoded SFP bits may be set to zero. It will be appreciated that the unused SFP bits could be used for particular purposes, e.g., to handle superframes consisting of more than thirty-two slots each or for Layer 1 power control messages. Also, the three unused SFP bits could be used, either alone or in combination with other unused (reserved) bits transmitted in each slot, for increasing the redundancy or strengthening the error correction coding of the SFP, if determined to be necessary. It will be appreciated that the SFP information could be included in the Layer 2 frame header information, rather than in separate Layer 1 fields as shown.

Also, in a system using thirty-two-slot superframes, it is currently preferred that the sixteen CRC, or check, bits in the Layer 2 frames sent in the BCCH slots are inverted, while the sixteen check bits in the Layer 2 frames sent in the SPACH slots are not inverted. Using the check bits in this way is advantageous in some situations where it is necessary to re-assign a mobile station to another paging slot. For example, if a system has been using twelve slots of a thirty-two-slot superframe for the BCCH and wants to use thirteen slots for the BCCH, mobile stations assigned to the first paging slot after the BCCH

-26-

slots must be informed that they should monitor another paging slot. The mobiles could obtain this information by decoding one or two bits that would identify the type of slot being decoded, but at a cost of reduced bandwidth. In Applicants' system, the mobile stations will recognize that something has
5 changed when they spot the inverted CRC bits, and in response they will re-read the F-BCCH, including the new DCCH structure message.

A hyperframe count and a primary SF indicator are also preferably included in the information carried by the BCCH slots; in particular as described in more detail below, these information elements are included in the DCCH
10 structure message carried by the F-BCCH. The hyperframe count identifies which hyperframe of a higher-level structure of paging frames and SMS frames is currently being broadcast, as described below in connection with FIG. 10. In accordance with Applicants' invention, four paging frame classes and/or a plurality of broadcast SMS sub-channels may be provided as described below.
15 The primary superframe indicator is a single bit that toggles to indicate whether the current superframe is the primary or the secondary superframe in the current hyperframe; when its value is zero, the current superframe may be the primary, and vice versa. In one embodiment of Applicants' invention, the hyperframe count counts modulo-12.

20 FIG. 9 shows a currently preferred partitioning of the Layer 2 user data bits before channel encoding. The DATA fields in the logical channels BCCH, SPACH, and RACH (normal and abbreviated) preferably use 1/2-rate convolutional encoding; thus, the two DATA fields in each forward DCCH slot carry 109 plaintext, or unencoded, BCCH or SPACH bits; and the two DATA
25 fields in each reverse DCCH slot carry either a normal 101 plaintext RACH bits or an abbreviated 79 plaintext RACH bits. Also, the encoded user data bits are preferably interleaved between the two DATA fields in each slot, but they are not interleaved among DATA fields in different slots in order to enable the longer sleep times available from Applicants' invention. Interleaving may be

-27-

done according to suitable convenient matrices, like those used under the IS-54B standard.

Different DCCHs may be assigned to different radio channel frequencies, and a different number of slots may be allocated to the BCCH on each DCCH.

- 5 Layer 2/3 information may also be different for each DCCH, but this is not required. In an embodiment in which each DCCH includes its own BCCH, much information is redundant from DCCH to DCCH, resulting in a loss of paging capacity. In another embodiment, DCCHs may be organized in master-slave relationships, in which full BCCH information would be available only on
10 the master DCCH; a mobile monitoring a slave DCCH would acquire its BCCH information by changing to its slave's corresponding master DCCH. It is currently preferred that each frequency carry a full set of BCCH information and a mobile station always acquire all its BCCH information on the same frequency as its assigned PCH channel.

- 15 The structure of the DCCH transmitted on the F-BCCH in the first slot of each superframe is the most important information for a mobile to acquire. An advantageous DCCH structure message comprises the information elements listed in the following table.

	Information Element	I E Type	Bit Length
20	Message type	M	8
	Number of F-BCCH slots	M	2
	Number of E-BCCH slots	M	3
	Number of S-BCCH slots	M	4
	Number of Skipped slots	M	3
25	E-BCCH change notification flag	M	1
	Hyperframe count	M	4
	Primary superframe indicator	M	1
	Number of DCCH slots on this frequency	M	2
	MAX_SUPPORTED_PFC	M	2
30	PCH_DISPLACEMENT	M	3

-28-

Additional DCCH frequencies	O	23-114
		Total = 33-147

M = Mandatory

O = Optional

As described above, the mobile station normally monitors only one of the PCH slots in a superframe to minimize power consumption, or battery drain. Since some paging messages may be longer than the capacity of a single time slot, each PCH slot carries a PCON bit that may be set to cause the assigned mobile station to read additional SPACH slots, the number of which is advantageously indicated by a parameter PCH_DISPLACEMENT sent on the F-BCCH. The additional slots to be read preferably are separated by at least 40 msec (one TDMA frame) from the assigned PCH slot for both full- and half-rate DCCHs. For example, for a full-rate DCCH, the mobile station would attempt to read every other SPACH slot up to the number indicated by the PCH_DISPLACEMENT parameter. This is advantageous in that it reduces the trunking loss caused by the creation of the several distinct paging channels. Also, using every other SPACH slot in this way gives a mobile station time for processing its received information to determine whether it must read additional slots. If every SPACH slot were used instead of at least every other one, a mobile station having a slow processing unit might not complete processing by the time the next SPACH slot occurred; since the mobile would not yet be aware that the PCON bit was set, it would have to read the next slot even if that were unnecessary and sleep mode performance would suffer.

Also, the transmission of long ARCH or SMSCH messages to a first mobile station may be interrupted to allow for the transmission of messages to a second mobile station. Each interruption of an ARCH or SMSCH message by another SPACH message may be limited to no more than a predetermined number n of time slots, or by Layer 3 timeout for SMSCH or ARCH messages. It will be understood that Layer 3 timeout refers to the common practice of

-29-

waiting for a response to a Layer 3 message only for a predetermined period. The number of interruptions each mobile station may suffer may also be limited.

Ordinarily, the probability of a successful transmission of a Layer 3 message is inversely related to the length of the message. Since the probability
5 can be quite small for long messages, a simple-minded system would spend much of its time re-transmitting or re-reading entire messages that were not properly received. In Applicants' system, Layer 3 paging and broadcast SMS messages are mapped onto Layer 2 frames, and these are organized in structures called
10 paging frames and SMS frames, respectively. For the BCCH, if a Layer 2 frame is not received properly, it is not necessary to re-read the entire Layer 3 message but only the improperly received Layer 2 frame. The ARCH and RACH can use ARQ.

In accordance with an aspect of Applicants' invention, the superframes and hyperframes on each DCCH are grouped into a succession of paging frames,
15 each of which includes an integer number of hyperframes and is a member of one of a plurality of paging frame classes; hence, the PCH slots have the paging frame structure. In accordance with one aspect of Applicants' invention, the mobile station reads its assigned PCH slot only in the hyperframes of its allocated paging frame class. (As described above, each mobile station is
20 allocated a specific PCH sub-channel within a paging frame based preferably on the mobile's IS-54B MIN identity.) In many cases, mobile stations would be allocated a paging frame class that would cause the mobiles to read their assigned PCH slots in each hyperframe; this minimizes call set-up time and sleep
25 duration. But other paging classes would have the mobiles read PCH slots in more widely separated hyperframes, delaying call set-ups but increasing sleep times to as much as 123 seconds for some types of paging frame structure. Thus, it will be appreciated that PCH slots are included in every superframe but the PCH slot assigned to a given mobile may not be.

Referring to the exemplary table shown in FIG. 10, primary and
30 secondary PCH slots p and s in the primary and secondary superframes,

-30-

respectively, of each hyperframe may be grouped in one of four PF classes PF_1 - PF_4 , which are distinguished by how frequently the PCH slot information is repeated. Class PF_1 may be called the "lowest" PF class because PCHs in this class repeat their information with the lowest duration between repeats; in
5 FIG. 10, the PCH slot is repeated in each successive hyperframe (i.e., in every successive superframe). Class PF_4 may be called the "highest" PF class because PCHs in this class repeat their information with the highest duration between repeats; in FIG. 10, the PCH slot is repeated only every fourth hyperframe. As described above, the PCH information in a primary superframe is guaranteed to
0 be repeated in the corresponding secondary superframe. In FIG. 10 for paging frame class $PF(i)$, where $i = 2, 3, 4$, only the PCH assignments which are aligned to HF_0 are shown for illustration purposes.

In the embodiment illustrated by FIG. 10, there are only four paging frame classes that are linearly related, yielding maximum sleep times of eight
15 superframes, or 5.12 seconds. Longer sleep times can be obtained by providing more classes that are exponentially related. For example, sleep times of 123 seconds are obtained in a system having eight paging frame classes in which the delays double from class to class. It will be understood that long sleep times can result in access delays that are unacceptable for typical telephone use; for
20 example, most callers attempting to reach a mobile would be unwilling to wait 123 seconds after dialing the mobile's number for contact to be established. Nevertheless, such delays may be tolerable in some cases, such as remote polling of equipment like soft-drink dispensers.

In an embodiment using the table illustrated in FIG. 10, the least common
25 multiple of the indices of the four paging frame classes is twelve; this is the reason that the HF counter counts modulo-12, as described above.

Three other terms used in describing the operation of the PF classes are default PF class, assigned PF class, and current PF class. The default PF class is the class assigned to the mobile station when its subscription to the system is
30 entered. If the default PF class happens to be higher than the highest class

-31-

supported by a DCCH, as defined by the parameter MAX_SUPPORTED_PFC in the DCCH structure message, the mobile would use the PF class defined by MAX_SUPPORTED_PFC. The assigned PF class refers to a PF class assigned to the mobile by the system, for example in the system's response to a registration request by the mobile. The PF class actually used during a communication may be called the current PF class.

According to other exemplary embodiments of the present invention, broadcast short message service (SMS) can be supported by way of logical sub-channeling in a variety of ways. Two examples will be discussed in detail, with other modifications and adaptations described after the detailed examples.

In one exemplary embodiment of Applicants' invention, depicted in FIGS. 11-13, the S-BCCH slots in successive superframes are grouped into a succession of fixed-length SMS frames, each preferably consisting of twenty-four superframes (twelve hyperframes) as shown in FIG. 11. This S-BCCH frame structure enables messages to be sent with highly variable periodicity without sacrificing capacity, and as described below, it avoids requiring the mobile stations to re-read constantly the entire S-BCCH information when only one of the many messages sent has changed. Also, choosing an SMS frame structure that is conveniently related to the paging frame class structure enables counters that are already in use for one purpose (paging) to be re-used for another purpose (SMS broadcast messaging).

The SMS frames are advantageously divided into a plurality of sub-channels, each having its own repetition cycle defined in terms of units of possible SMS frames. For most practical situations, the sub-channel repetition time should not be too long. In a manner similar to the handling of the F-BCCH change flag described above, a mobile station is informed of a change in the contents of particular sub-channels through an SMS transition flag (TF) included in its PCH slot information.

Currently, four SMS sub-channels are preferred for this exemplary embodiment, and the SMS sub-channels are sub-multiplexed on the S-BCCH

-32-

channel in units of SMS frames, e.g., SMS frame SMS(i), where $i = 1, \dots, N$, as illustrated in FIG. 12. It will be understood that each (Layer 1) time slot carries a respective SMS frame and that a Layer 3 SMS message can span several SMS frames.

5 An SF number is advantageously derived from the hyperframe count and primary superframe indicator sent on the BCCH as follows:

$$\text{SF number} = 2 * \text{HF count} + \text{primary SF indicator}.$$

The first S-BCCH slot(s) within each SMS frame (superframe 0) would contain a header that describes the structure of the SMS sub-channel. As noted above, the
10 number of superframes within each SMS frame is fixed for this exemplary embodiment, and thus the number of slots assigned to the SMS frame are 0, 24, 48, 72, . . . (full-rate), depending on how many slots per superframe are assigned to S-BCCH. The SMS frame is aligned to start at HF counter equal to zero and in a primary superframe to help the mobile synchronize to the SMS
15 frame structure. In this way, SMS frames are synchronized to the hyperframes and superframes, although it will be appreciated that the start of an SMS frame is offset from the start of a hyperframe (or a primary superframe) since the S-BCCH slots are not the first slots in a superframe. Furthermore, regardless of how many paging frame classes are supported, the system increments the
20 hyperframe count to provide SMS frame synchronization information to the mobile station.

According to Layer 2 information found in every first slot in each SMS frame, the set of messages in an SMS frame SMS(i) may span a number $M(i)$ of
25 SMS frames before a cycle is completed. Regardless of varying message set cycles among the sub-channels, SMS frame SMS(i) is always followed by SMS frame SMS($(i+1) \bmod N+1$) in order of transmission in this exemplary embodiment. Thus, Layer 3 broadcast SMS messages can span several SMS frames, which represents a tradeoff between the number of slots in each superframe devoted to SMS broadcast and the time needed for message
30 transmission.

-33-

A transition flag (TF) is provided for each SMS sub-channel, and the flags for all SMS sub-channels are submultiplexed onto a single flag, transmitted on the SPACH channel, that points to the next logical SMS frame to be read. For example, FIG. 12 shows flag TF(2) pointing to SMS frame SMS(2). If the transition flag for a sub-channel indicates a change, the mobile station reads an S-BCCH header field at the start of the next logical SMS frame to obtain further information, as described more fully below.

Header information describes the sub-channeling of the broadcast SMS channel and is provided in the first slot of every SMS frame. The mobile can also find the Layer 3 structure of the SMS frame associated with this header. A suitable SMS Header information element located at the start of every SMS frame is shown in the table below.

Information Element	Range (Logical)	Bits
Number of Sub-channels	1-4	2
Sub-channel Number	1-4	2
Phase Length of Sub-ch. Cycle	1-64	6
Phase Number of Sub-ch. Cycle	1-64	6
Number of SMS Messages (N)	1-64 (set to 1 plus value in field)	6
<ul style="list-style-type: none"> ◦ SMS Message ID (Note 1) ◦ Layer 2 Frame Start (Note 1) 	<ul style="list-style-type: none"> 0-255 (unique ID in cycle) 0-255 (Layer 2 frame identifier) 	<ul style="list-style-type: none"> 8 8

Note 1: N instances of these two elements are sent consecutively.

SMS data may span several SMS frames, but the flags TF enable interruption of the sub-channel cycles (cycle clearing). For example, after a flag TF, the mobile station assumes that the next sub-channel is the start of the new cycle. There are two ways to change the data provided on the broadcast SMS: changing the Layer 3 messages within the SMS (messages may be added and/or

-34-

deleted from any position in the cycle), and changing the structure of the sub-channels.

5 The SMS Message IDs, of which there are a set of 256, and their associated Layer 2 Frame Starts comprise a list of all messages appearing in an SMS frame. SMS Message IDs are unique for each SMS frame and the whole
set of 256 values is used before the set begins to be used again in order to aid the mobile in searching for changed message(s) and in avoiding reading messages that have not changed. A Layer 2 Frame Start information element is provided to point to the start of the Layer 2 frame in which the associated SMS message
0 begins (the message does not have to begin at the start of the Layer 2 frame). A description of message delivery is provided in the description of the S-BCCH Layer 2 Protocol given below.

5 In the example shown in the table below, four messages make up SMS frame 1, and it may be assumed that only one slot in each superframe is dedicated to S-BCCH. (Since it is currently preferred that each SMS frame include twenty-four superframes, there are twenty-four slots in each SMS frame.)

-35-

Previous SMS Frame 1 Header				New SMS Frame 1 Header			
5	Number of sub-channels		3	Number of sub-channels		3	
	Sub-channel number		1	Sub-channel number		1	
	Length of sub-ch. cycle		2	Length of sub-ch. cycle		2	
	Phase of sub-ch. cycle		1	Phase of sub-ch. cycle		1	
	Number of SMS messages (N)		4	Number of SMS messages (N)		5	
10	◦1	SMS message ID	1	◦1	SMS message ID	1	
	◦1	Layer 2 Frame Start	1	◦1	Layer 2 Frame Start	1	
	◦2	SMS message ID	2	◦2	SMS message ID	2	
	◦2	Layer 2 Frame Start	2	◦2	Layer 2 Frame Start	2	
15	◦3	SMS message ID	3	◦4	SMS message ID	4	
	◦3	Layer 2 Frame Start	2	◦4	Layer 2 Frame Start	2	
	◦4	SMS message ID	4	◦5	SMS message ID	5	
	◦4	Layer 2 Frame Start	3	◦5	Layer 2 Frame Start	3	
				◦6	SMS message ID	6	
				◦6	Layer 2 Frame Start	3	

In the table above, the mobile is assumed to be monitoring the SPACH when the TF toggles to indicate a change in the S-BCCH. The mobile knows from its own internal superframe count where the start of the SMS frame is, and it can determine that SMS sub-channel three is currently being broadcast by reading the SMS header and that the TF points to a change in SMS sub-channel one. When SMS sub-channel one begins, the mobile reads the SMS header. It determines that message 3 is removed; that the position of message 4 has changed (but the message ID is the same so the mobile does not need to re-read this message); and that new messages 5 and 6 have been added and must be read.

The mobile may skip the appropriate number of Layer 2 frames to read the new messages.

S-BCCH Layer 2 PROTOCOL

The S-BCCH Layer 2 protocol is used when a TDMA burst carries S-BCCH information. Each S-BCCH Layer 2 protocol frame is constructed to fit in a 125-bit envelope. An additional five bits are reserved for use as tail bits, which are the last bits sent to the channel coder, resulting in a total of 130 bits of Layer 2 information carried within each S-BCCH slot. As noted above, the Layer 2 protocol for S-BCCH operation supports only unacknowledged operation. Several different S-BCCH Layer 2 frames which support this exemplary SMS embodiment are shown in FIGS. 13a, 13b, 13c.

FIG. 13a shows a mandatory minimum S-BCCH BEGIN frame and FIG. 13b shows another S-BCCH BEGIN Frame used when two Layer 3 messages are included in the frame with the second Layer 3 message being continued in a following frame. The BEGIN frames are used for starting the delivery of one or more Layer 3 messages on the S-BCCH, and it is currently preferred that an S-BCCH BEGIN frame be used as the first frame of the S-BCCH cycle. If the first Layer 3 message is shorter than one S-BCCH frame, a begin/end indicator BE is added to the end of the L3DATA field as shown to indicate whether or not an additional Layer 3 message is started within the BEGIN frame. As shown in FIG. 13a, if the BE indicator is set to indicate "END", the rest of the BEGIN frame is padded with FILLER, e.g., zeroes. As shown in FIG. 13b, if the BE indicator is set to indicate "BEGIN", a new Layer 3 message is started in the BEGIN frame. If the L3DATA field ends on an S-BCCH frame boundary, the BE indicator is not included in the frame; an "END" indication is implied. If the L3DATA field ends with less than nine bits remaining in the S-BCCH frame, the BE indicator is set to "END", and the rest of the frame is padded with FILLER.

-37-

FIG. 13c shows an S-BCCH CONTINUE Frame (mandatory minimum), which is used for continuation of a Layer 3 message that was too long to fit into the previous frame. The continuation length indicator CLI field indicates how many bits of the CONTINUE frame belong to the continued message, and thus the preceding Layer 3 message may have to be padded with FILLER. If the BE indicator is set to "END", the rest of the CONTINUE frame is padded with FILLER. If the BE indicator is set to "BEGIN", a new Layer 3 message is started in the CONTINUE frame. If the L3DATA field ends on an S-BCCH frame boundary, the BE indicator is not included in the frame; an "END" indication is implied. If the L3DATA field ends with less than nine bits remaining in the S-BCCH frame, the BE indicator is set to "END", and the rest of the frame is padded with FILLER.

The CLI makes it possible for mobile stations to receive any message starting in a continuation frame, even if the preceding logical frame was not received. The following table summarizes the fields included in the S-BCCH Layer 2 protocol frames.

-38-

5

Field Name	Bit Length	Values
SCS = S-BCCH Cycle Start	1	0 = Not the start of an S-BCCH cycle 1 = Start of an S-BCCH cycle
BC = Begin / Continue	1	0 = Begin 1 = Continue
CLI = Continuation Length Indicator	7	Number of bits remaining in previous Layer 3 message.
L3LI = Layer 3 Length Indicator	8	Variable length Layer 3 messages supported up to a maximum of 255 octets
L3DATA = Layer 3 Data	Variable	Contains a portion (some or all) of the Layer 3 message having an overall length indicated by L3LI. The portion of this field not used to carry Layer 3 data is filled with zeroes.
BE = Begin / End	1	0 = Beginning 1 = End
FILLER = Burst Filler	Variable	All filler bits are set zero
CRC = Cyclic Redundancy Code	16	Same generator polynomial as IS-54B. The nominal DVCC is applied in the calculation of CRC for each S-BCCH Layer 2 frame.

10

Similar logical frames can be defined for the F-BCCH and E-BCCH, as described in U.S. Patent Application No. 08/147,254 for example, but these are beyond the scope of this application.

Layer 3 MESSAGES

The S-BCCH Layer 3 messages that are mapped to the Layer 2 frames are described below. In all messages shown in tabular form below, the information elements in the top rows of the tables are preferably the first elements to be delivered to Layer 2. In the information elements, the most significant bit (the left-most bit in the tables) is the first bit to be delivered to Layer 2. The information elements are described in alphabetical order after the description of the messages below.

There are two types of S-BCCH messages used for SMS broadcast: SMS frame header messages; and SMS non-header messages, which are those used to transfer the actual messages to the mobile stations.

The SMS frame header messages describe the structure of the SMS sub-channel, and are provided in the first slot of each SMS frame. The format of a suitable SMS frame header message is described in the following table.

Information Element	Type	Bit Length
Message Type	M	8
Number of Sub-channels	M	2
Sub-channel Number	M	2
Phase Length of Sub-ch. Cycle	M	6
Phase Number of Sub-ch. Cycle	M	6
Number of SMS Messages (N)	M	6
◦ SMS Message ID (Note 1)	M	8
◦ Layer 2 Frame Start (Note 1)	M	8
		Total = 46

NOTE 1: N instances of these two elements are sent consecutively.

The format of a suitable SMS non-header, broadcast message is as follows:

-40-

Information Element	Type	Bit Length
Message Type	M	8
SMS Message ID	M	8
Text Message Data Unit	M	N*8 N max. = 253

5 In one aspect of Applicants' invention, SMS messages may be encrypted in a way that supports different classes of message service, much like cable television systems distinguish premium classes of service from a basic service class by scrambling or otherwise protecting the premium programming. For example, three classes might be provided as follows: a basic class in which any
10 subscriber paying an appropriate fee would be able to de-crypt some of the SMS broadcast messages, such as product advertisements, weather and vehicle traffic announcements; a higher class in which a subscriber paying a higher fee would be able to de-crypt the SMS broadcast messages available to the basic class and additional messages, such as news items; and a highest class in which a
15 subscriber paying a highest fee would be able to de-crypt all of the SMS broadcast messages, including financial quotations and higher-value items of information.

The de-cryption of the SMS messages could be carried out by the processing units in the mobile stations according to any of a wide variety of
20 cryptographic techniques. Preferably, each broadcast message would include as an attribute an indicator for determining which encryption key or algorithm should be used to decode the respective message. Such attributes might be included in the SMS frame headers, and the encryption keys or algorithms could be sent to the mobiles over the air or entered directly, via a "smart card", for
25 example. As an alternative, the sub-channels could be individually encrypted, so that broadcast SMS messages included in the time slots of one of the SMS sub-channels are encrypted according to one encryption method and the broadcast

-41-

SMS messages included in the time slots of another SMS sub-channel are encrypted according to a another encryption method.

INFORMATION ELEMENT DESCRIPTION

- 5 A few coding rules apply to the information element descriptions. For example, information elements of the type "flag" have values of 0 to indicate "disable", or "off", or "false", and values of 1 to indicate "enable", or "on", or "true". Also, certain BCCH fields do NOT trigger a transition in the BCCH change flag in the SPACH; those fields are designated as non-critical, or "NC".
- 10 Information elements of the type "transition" are modulo-1 counters for indicating changes in current status. The channel number is coded in accordance with the IS-54B standard, unless otherwise noted. All lengths are specified in bits, unless otherwise noted.

Layer 2 Frame Start

- 15 This variable indicates the number of slots from the start of the SMS sub-channel cycle to the beginning of the SMS message, which may not begin in the indicated SMS slot but may be contained in an end/begin burst used to start delivery of this message.

-42-

Message Type

This 8-bit information element identifies the function of the message being sent. The message types are coded as follows:

S-BCCH Messages	Code (binary-hex)
Broadcast Information Message	0010 0111 - 27

5

Number of SMS Messages

This variable indicates the number of broadcast SMS messages in this SMS frame (1 plus the value in this field).

Number of Sub-channels

- 10 This variable indicates the number of SMS sub-channels being used by this DCCH (1 plus the value in this field).

Phase Length of Sub-ch. Cycle

This variable indicates the number of SMS frames that make up one cycle (1 plus the value in this field).

- 15 Phase Number of Sub-ch. Cycle

This variable indicates which SMS frame in the cycle is currently being broadcast.

Sub-channel Number

- 20 This variable indicates which sub-channel is currently being broadcast.
- According to another exemplary embodiment, the amount of bandwidth per sub-channel (i.e., the periodicity at which each sub-channel is transmitted) and the ordering of sub-channels is dynamic to provide additional flexibility to broadcast SMS systems. Although the term "sub-channels" is used herein, those skilled in the art will appreciate that any other term or phrase which connotes logical grouping of SMS messages could be used to describe these groupings of the present invention. Moreover, according to this exemplary embodiment, a greater number of SMS sub-channels, e.g., 8, 16, 32, 64, etc., can be supported than the four sub-channels used to illustrate the previous exemplary embodiment.
- 25

-43-

For the purposes of illustration, rather than limitation, an example will be provided wherein up to 32 S-BCCH sub-channels are supported.

According to this exemplary embodiment, a particular subset of message attributes is associated with each sub-channel rather than broadcasting messages having any set of attributes on any sub-channel, as in the previous exemplary embodiment. The particular order in (and periodicity at) which these sub-channels are transmitted can be varied by the system operator according to, for example, the number of messages which have the attribute(s) associated with each sub-channel. The system can broadcast messages using associated with a sub-channel on, for example, a number of contiguous S-BCCH time slots, which number may vary for each sub-channel. The broadcasting of a sub-channel may, however, be interrupted by the system in order to broadcast messages on sub-channels 0 and 1 for reasons that will become apparent.

Since sub-channeling according to this exemplary embodiment does not have a fixed, time multiplexed format such as that provided in the earlier embodiment, a different mechanism (i.e., other than an SMS frame header) is used to provide overhead information. In this example overhead information including, for example, the total number of sub-channels currently activated, the message encryption algorithm associated with each sub-channel (if any), the user group associated with each sub-channel (if any), and other S-BCCH attributes described below, is provided on sub-channel 0. Channel 0 is dedicated to this overhead function so that mobile stations will know where to find this information. When a cycle of sub-channel 0 information is to be sent by the system (e.g., broadcast from a base station), it can be started in a first S-BCCH time slot coincident with a hyperframe counter value of zero. For example, sub-channel 0 can be broadcast at least once every $12 \cdot N$ hyperframes ($N=1,2,3,\dots$) or when otherwise desired by a system operator. Once started, the broadcast of sub-channel 0 should be completed without interruption using consecutive S-BCCH time slots.

-44-

Sub-channel 1 is dedicated, according to this exemplary embodiment, to the provision of messages associated with other sub-channels (i.e., sub-channels 2-31 in this example) that have recently been changed or added. Typically, deleted messages are of no interest to mobile stations, however, those skilled in the art will recognize that the present invention can be readily extended to provide an indication to mobile units that a message has been deleted in a manner similar to that described herein for changed messages and added messages. The broadcast of sub-channel 1 by the system may commence after the completion of any sub-channel or by interrupting a sub-channel (other than sub-channels 0 or 1). For example, it may be considered desirable by a system operator to begin increase the periodicity of transmission of sub-channel 1 after the transmission of sub-channel 0 in which a change or changes have been indicated. Once the broadcast of sub-channel 1 has begun, it should be completed without interruption using consecutive S-BCCH time slots. By reading sub-channel 1, a mobile station will be able to quickly access changed or added messages of interest.

From the mobile station's perspective, upon camping on a DCCH the mobile can, for example, read sub-channel 0 to determine if it needs to acquire the S-BCCH information broadcast thereon that is associated with that particular DCCH. For example, after cell reselection, the mobile may have camped on a DCCH whose S-BCCH has a different structure in terms of the number of sub-channels currently activated, the user groups and/or encryption techniques associated with each sub-channel, etc. In such a case, the mobile would need this information in order to perform additional SMS activities supported by that DCCH. The selective acquisition of S-BCCH information is supported by, for example, a broadcast domain indicator provided as part of a Layer 3 message transmitted on sub-channel 0. This broadcast domain indicator is discussed in more detail below. For example, a mobile station reading sub-channel 0 may determine that it has locked to a DCCH associated with the same broadcast domain under which that mobile was previously operating, i.e., if the broadcast

-45-

domain value read by the mobile station is the same as that previously read and stored, but where some changes have occurred in the S-BCCH information. In such a situation, the mobile station may need to read only the S-BCCH information which has changed since certain sub-channeling structure will be
5 common to cells which support the same broadcast domain. More detailed examples describing of the interaction between a mobile station reading sub-channel 0 and the broadcast domain indicator will be provided after a description of the Layer 2 protocols and Layer 3 messages.

While in the process of acquiring the S-BCCH information broadcast on
10 sub-channel 0, this information could be changed by the system, e.g., to add a new sub-channel to handle messages sent to a new user group and/or using a different encryption algorithm. Similarly, the S-BCCH information associated with a DCCH can change after it is acquired by a mobile station. In either case a Layer 2 change indication is sent to the mobile which responds by reading sub-
15 channel 0. For example, a change notification bit can be placed in the SPACH header and used to notify mobile stations of changes in the content of the S-BCCH information. For a detailed description of the SPACH and SPACH header, the interested reader is referred to U.S. Patent Application Serial No. 08/331,816 entitled "Layer 2 Protocol in Cellular Communication System" filed
20 on October 31, 1994, which disclosure is incorporated here by reference.

According to this exemplary embodiment, and as distinguished from the transition flags TF(i), change indication is generic in the sense that the particular sub-channel or sub-channels which have been modified are not identified in the Layer 2 change notification. Instead, the affected mobile stations will read sub-
25 channel 0 to determine the specific sub-channel or sub-channels which have been modified. In this way the modified S-BCCH information can be sent to the mobile stations beginning in the hyperframe immediately following the hyperframe in which the Layer 2 change indication is provided.

The exemplary Layer 2 protocol defined below supports S-BCCH
30 operation to allow a mobile station to uniquely determine the start and end of a

-46-

sub-channel and to begin reading a sub-channel starting with any Layer 2 frame belonging to that sub-channel. According to this exemplary embodiment, each sub-channel is sent using up to 256 Layer 2 frames. Of course, those skilled in the art will appreciate that other sub-channel capacities can be used without departing from the spirit of the present invention. An exemplary 256 Layer 2 frame sub-channel would, however, provide about 10 maximum length (i.e., 255 octets) Layer 3 messages per sub-channel or about 25 SMS messages per S-BCCH sub-channel assuming an average of 100 octets of data per message. In this exemplary embodiment, a Layer 3 message qualifier can be used to identify up to, for example, 256 distinct S-BCCH Payload messages over all of the SMS "traffic" sub-channels 2-31. Additional S-BCCH messages can be identified by creating other types of Layer 3 messages and pairing the associated Layer 3 message type with the Layer 3 message qualifier e.g., 256 different S-BCCH messages per pair. Having provided an overview of message delivery in accordance with this second exemplary SMS embodiment, exemplary Layer 2 and Layer 3 protocols for supporting these functions will now be described.

S-BCCH LAYER 2 PROTOCOL (Second Exemplary Embodiment)

The S-BCCH Layer 2 protocol is used when a TDMA slot is used to carry S-BCCH information. The S-BCCH protocol allows for supporting up to a maximum of 32 distinct S-BCCH sub-channels. The set of layer 3 messages comprising a S-BCCH sub-channel is sent using up to 256 S-BCCH layer 2 protocol frames.

Each S-BCCH Layer 2 protocol frame can be constructed to fit within a 125 bit envelope. An additional 5 bits are reserved for use as tail bits resulting in a total of 130 bits of information carried within each S-BCCH slot. The Layer 2 protocol defined in this exemplary embodiment for S-BCCH operation supports only unacknowledged operation. Figures 14(a)-14(e) provide examples of Layer 2 S-BCCH frames.

-47-

The BEGIN frame is used for starting the delivery of one or more Layer 3 messages on any given sub-channel of the S-BCCH. The Layer 3 that constitutes the opening message of a full cycle of S-BCCH information for any sub-channel shall be transmitted starting with a BEGIN FRAME and shall occupy the first L3DATA field included in the BEGIN frame should more than one
5 L3DATA field be present therein. Exemplary rules for the placement of Layer 3 messages within a BEGIN frame are as follows.

If a Layer 3 message fits entirely within the L3DATA field of a BEGIN frame with 9 or more bits remaining in the frame, the Begin Indicator (BI) is
10 included immediately after the L3DATA field to indicate whether or not an additional Layer 3 message is started within the frame. If BI=0, no other Layer 3 message is started and the rest of the frame is padded with FILLER. If BI=1 a L3LI field is included immediately after the BI field. The L3LI field is then followed by another L3DATA field containing a portion of the new Layer 3
15 message determined by the number of bits remaining in the frame.

If, on the other hand, a Layer 3 message fits entirely within the L3DATA field of a BEGIN frame with from 1 to 8 bits remaining in the frame and another Layer 3 message is to be sent, BI=0 is included immediately after the L3DATA field. The rest of the frame is then padded with FILLER and the next Layer 3
20 message is sent starting with another BEGIN frame. If a Layer 3 message fits entirely within the L3DATA field of a BEGIN frame with from 1 to 8 bits remaining in the frame and no other Layer 3 message is to be sent, BI=0 is included immediately after the L3DATA field and the rest of the frame is padded with FILLER. If a Layer 3 message fits entirely within the L3DATA field of a
25 BEGIN frame with no bits remaining, the BI field is not present and the end of the Layer 3 message is implied. This case is exemplified in Figure 14a.

Lastly, if a Layer 3 message does not fit entirely within the L3DATA field of a BEGIN frame, it is completed using as many CONTINUE frames as necessary. The other fields illustrated in FIG. 14a are described in Table 1
30 below.

-48-

The CONTINUE frame is used whenever a Layer 3 message cannot be completed within the previous S-BCCH Layer 2 frame. Exemplary CONTINUE frames are illustrated in FIGS. 14b-14d. The CLI field indicates how many bits of the CONTINUE frame belong to the continued Layer 3 message. This in turn allows for mobile stations to receive a portion of a new message which may be present in the CONTINUE frame following the L3DATA field used to complete a message continued from the previous frame. Exemplary rules for the placement of Layer 3 message information within a CONTINUE frame are as follows.

10 If the CLI field indicates that the remainder of a continued Layer 3 message fits entirely within the CONTINUE frame with 9 or more bits remaining in the frame, the Begin Indicator (BI) is included immediately after the L3DATA field to indicate whether or not an additional Layer 3 message is started within the frame. For example, if BI=0 no other Layer 3 message is started and the rest of the frame is padded with FILLER. This case is illustrated as FIG. 14b.

15 If BI=1, then an L3LI field is included immediately after the BI field. The L3LI field is then followed by another L3DATA field containing a portion of the new Layer 3 message. The length of the portion of the new Layer 3 message in the second L3DATA field is determined by the number of bits remaining in the frame. This case is illustrated in FIG. 14c.

20 If CLI indicates that the remainder of a continued Layer 3 message fits entirely within the CONTINUE frame with from 1 to 8 bits remaining in the frame and another Layer 3 message is to be sent, BI=0 is included immediately after the L3DATA field. The rest of the frame is padded with FILLER and the next Layer 3 message is sent starting with another BEGIN frame. This case is also exemplified by the format of FIG. 14b.

25 If CLI indicates that the remainder of a continued Layer 3 message fits entirely within the CONTINUE frame with from 1 to 8 bits remaining in the frame and no other Layer 3 message is to be sent, BI=0 is included immediately after the L3DATA and the rest of the frame is padded with FILLER. If CLI

30

indicates that the entire CONTINUE frame contains information belonging to a continued Layer 3 message, the BI field is not present in the frame. This is illustrated in FIG. 14d.

- 5 A continued Layer 3 message is completed using as many CONTINUE frames as necessary. The following table summarizes the exemplary fields provided in these S-BCCH Layer 2 frames according to this exemplary embodiment.

TABLE 1: S-BCCH Layer 2 Protocol Field Summary

	FIELD NAME	LENGTH (Bits)	VALUES
10	BC = Begin/Continue	1	Identifies the type of L2 frame (0 = Begin, 1 = Continue)
	SID = Sub-channel ID	5	Uniquely identifies the sub-channel that a L2 frame belongs to (0..31).
	FDC = Frame Down Counter	8	Uniquely identifies a Layer 2 frame used in sending a cycle of sub-channel information (0..255).
15	SSI = Sub-channel Start Indicator	1	Indicates whether or not a L2 frame is the first frame used in sending a cycle of sub-channel information (0 = No, 1 = Yes).
	SCN = S-BCCH Change Notification	1	Transitions whenever there is a change in the content of S-BCCH information. A mobile station responds by reading S-BCCH information on sub-channel 0.
	CLI = Continuation Length Indicator	7	Number of bits in the current L2 frame used to carry information from a previously initiated L3 message.

-50-

FIELD NAME	LENGTH (Bits)	VALUES
L3LI=Layer 3 Length indicator	8	Variable length Layer 3 messages supported from 0 up to a maximum of 255 octets.
L3DATA=Layer 3 Data	Variable	Contains a portion (some or all) of the Layer 3 message having an overall length as indicated by L3LI. The portion of this field not used to carry Layer 3 information is filled with zeros.
BI=Begin Indicator	1	0=No additional Layer 3 message present 1=Additional Layer 3 message present
FILLER=Burst Filler	Variable	All filler bits are set to zero.
CRC=Cycle Redundancy Code	16	Same generator polynomial as IS-54B. The nominal DVCC is applied in the calculation of CRC for each S-BCCH Layer 2 frame.

- 5 An S-BCCH Request primitive can be provided to transfer Layer 3 messages to be sent on the S-BCCH to Layer 2. For example, the S-BCCH Request primitive can include the following protocol elements:
- 10 (1) a Layer 3 message (examples below);
 - (2) a Layer 3 Length Indicator (L3LI) providing the length of the Layer 3 message (e.g., in octets); and
 - 15 (3) a sub-channel ID which identifies the sub-channel that the Layer 3 message is associated with.

LAYER 3 MESSAGES (Second Exemplary Embodiment)

Exemplary Layer 3 messages which can be mapped to Layer 2, e.g., using the primitive described above are set forth below. As in the description of

-51-

the previous exemplary embodiment, the information elements in the top rows of tables can be the first elements delivered to Layer 2. In the information elements, the most significant (i.e., leftmost) bit is the first bit to be delivered to Layer 2. The information elements are described in alphabetical order after the description of the message below.

A **Sub-channel Configuration** message is sent on sub-channel 0 to define the format of supported channels. An exemplary format for the **Sub-channel Configuration** message is illustrated below.

Information Element	Reference	Type	Length
Protocol Discriminator		M	2
Message Type		M	6
Sub-channel Count (N)		M	5
Sub-channel Info (Note 1)		O	13-*

Note 1: N instances of this information element are included up to a maximum number of supported "traffic" subchannels, e.g., 30.

The **Sub-channel Count** information element identifies the number of sub-channels used in support of sending S-BCCH information. In this exemplary embodiment five bits are provided to support the 32 sub-channels. Of course more or fewer bits could be provided to represent this value if more or fewer sub-channels are to be supported, respectively.

The **Sub-Channel Info** information element identifies the attributes of supported S-BCCH sub-channels. An exemplary format for this information element is shown below.

-52-

Field	Length
Sub-channel ID (Note 1)	5
MEA	3
MEK	3
Wildcard Indicator	1
Broadcast Mode	1
User Group Type (Note 2)	0,2
User Group ID (Note 2)	0,20,24,34 or 50

Note 1: Sub-channels 0 and 1 are defined implicitly and therefore need not be explicitly defined.

Note 2: Only present if the Broadcast Mode indicates User Group ID specific broadcast.

Each of the fields of the **Sub-channel Info** information element and the attributes which they describe are set forth in more detail below.

The **Sub-channel ID** field identifies a specific S-BCCH sub-channel (0..31) associated with each of the other parameters in the information element. This field can be used by a mobile station as an index by which the mobile station can update its information as to the structure of certain sub-channels as needed, e.g., newly added sub-channels.

The **MEA** and **MEK** fields identify the encryption technique (if any) associated with the particular sub-channel identified by the sub-channel ID field. Encryption can, for example, be one of the message attributes upon which the grouping of messages into logical sub-channels can be based. The **MEA** field can, for example, be coded as follows.

-53-

Value	Function
000	No Message Encryption
001	Message Encryption Algorithm A
All other values are reserved	

5 The **MEK** field can, for example, be coded as follows.

Value	Function
001	Message Encryption Key A
All other values are reserved	

10 The combination of both an **MEA** and **MEK** can be used to provide, for example, different levels of service to publicly available channels. For example, different encryption algorithms could be associated with each encryption key to provide different levels of access to information. Thus, a Bronze class message group could be associated with a first encryption algorithm and an encryption key, a Silver class message group (i.e., sub-channel) could be associated with a second encryption algorithm and that encryption key, and a Gold class message group could be associated with a third encryption algorithm and that encryption key.

15 The **Wildcard Indicator** field indicates whether or not the sub-channel identified by the sub-channel ID field belongs to the broadcast domain. Each broadcast domain (e.g., each system operator) may have certain standard or common sub-channels. Other sub-channels, which are not common to a broadcast domain, may nonetheless be broadcast by the system. The mobile station learns of these non-standard sub-channels by reading the **Wildcard Indicator**. The **Wildcard Indicator** field can, for example, be coded as follows.

-54-

Value	Function
0	Standard Sub-channel (part of Broadcast Domain)
1	Wildcard Sub-channel (not part of Broadcast Domain)

5 The **Broadcast Mode** field indicates whether or not the sub-channel identified in sub-channel ID field is restricted to a particular user group. The **Broadcast Mode** field can, for example, be coded as follows.

Value	Function
0	Unrestricted Broadcast
1	User Group ID Specific Broadcast

10 The **User Group Type** and **User Group ID** fields specify the user group to which this sub-channel is restricted if the appropriate value is set in the Broadcast Mode field. The **User Group Type** field can, for example, be coded as follows.

15

Value	Function
00	20-bit Local UGID
01	24-bit SOC UGID
10	34-bit National UGID
11	50-bit International UGID

20 The **User Group Type** field indicates, for example, how many bits to expect in the **User Group ID** field, which identifies the User Group to which an S-BCCH sub-channel has been allocated.

-55-

The **Sub-channel Change Summary** message is also sent on S-BCCH sub-channel 0 to indicate the nature of changes made to S-BCCH information. An exemplary format for this message is set forth below.

Information Element	Reference	Type	Length
5 Protocol Discriminator		M	2
Message Type		M	6
Broadcast Domain ID		M	8
Change Indicator Map		M	32
Change Acquisition Map		M	32

10 The **Broadcast Domain ID** information element is used to identify, for example, a system operator code (SOC) specific S-BCCH broadcast area as described above. More specifically, the **Broadcast Domain ID** provides an indication to a mobile station of whether certain commonalities expected within a broadcast domain are available to that mobile station when the mobile station
 15 locks on to another DCCH. For example, adjacent DCCHs that have the same SOC and that send the same set of S-BCCH information on the same standard sub-channels shall use the same **Broadcast Domain ID** value.

The **Change Indicator Map** information element is used to provide change indication information on a per sub-channel basis. The leftmost bit in
 20 this map corresponds to sub-channel 31 and the rightmost bit corresponds to sub-channel 0. Whenever there is a modification to the content of a sub-channel (other than a deletion) the corresponding bit position in this map is toggled. Mobile stations need only proceed to acquire the new S-BCCH information for the modified sub-channels that are of interest, e.g., according to the **Change**
 25 **Acquisition Map** element described below.

The **Change Acquisition Map** information element is use to provide change acquisition information on a per sub-channel basis. The leftmost bit in

-56-

this map corresponds to sub-channel 31 and the rightmost bit corresponds to sub-channel 0. Whenever there is a modification to the content of a sub-channel (other than a deletion) the corresponding bit position in this map is used to inform mobile stations how to acquire the new information as follows. When a bit of this map is set to 0, then mobile stations that have previously read the newly modified sub-channel associated with that bit shall acquire the new information by reading sub-channel 1. Mobile stations that are in the process of reading or have never read the newly modified sub-channel shall acquire the new information by (re-)reading a full cycle of information from the modified sub-channel. When a bit of this map is set to 1, mobile stations shall acquire the new information by reading a full cycle of information from the newly modified sub-channel.

The **S-BCCH Payload** message is sent on sub-channels 1 through 31 in order to provide the Layer 3 messages specific to S-BCCH operation and can, for example, have the following format.

Information Element	Reference	Type	Length
Protocol Discriminator		M	2
Message Type		M	6
Message Type Qualifier		M	8
Other Data (TBD)		TBD	TBD

The **Message Type** information element identifies the function of the message, e.g., an S-BCCH Payload message. The **Message Type Qualifier** information element is used to identify up to 256 distinct S-BCCH messages. For example:

-57-

Value	Function
0000 0000	Casino Clips
0000 0001	Road Report
0000 0010	Rugby News
All other values are reserved.	

5

The **Other Data (TBD)** field can be used to provide, e.g., higher layer protocols such as how long a message should be retained for retransmission on a sub-channel.

10 The **Sub-channel Delimiter** message can be sent on sub-channel 1 to delimit groups of S-BCCH Payload messages, also sent on sub-channel 1, that are associated with specific sub-channels. This allows mobile stations to determine the nominal sub-channels that each S-BCCH Payload message is associated with. The **Sub-channel Delimiter** message can, for example, have the following format.

15

Information Element	Reference	Type	Length
Protocol Discriminator		M	2
Message Type		M	6
Sub-channel ID		M	5

20 Having described exemplary Layer 3 messages, the operation of a mobile station in such a system will now be described by way of several examples. As mentioned above, a mobile station that acquires a new DCCH (e.g., by cell reselection) shall perform an S-BCCH update by first reading sub-channel 0 to determine if the S-BCCH information associated with this DCCH is different. For example, assume that the mobile station has travelled to a cell whose DCCH
25 is associated with another broadcast domain (e.g., a different system operator).

-58-

Under these circumstances, the mobile station will read a full cycle of information on all sub-channels determined to be of interest according to subchannel 0 information. Sub-channels of interest can, for example, include those sub-channels whose encryption techniques match those which the mobile station can decrypt and/or those sub-channels accessible to a common user group supported by the mobile station.

As another example, consider a mobile station which is informed, by a change in the notification flag found in the SPACH header, that the contents of the S-BCCH have changed. Suppose, for this example, that the change constitutes the addition of a new sub-channel. The mobile station will then read sub-channel 0. If it first receives a **Subchannel Change Summary** message, the mobile station will learn, from the setting of a bit in the **Change Indicator Map** information element, that a new sub-channel has been added. However, the mobile station will not know, based on this message, whether or not this is a sub-channel of interest, since the **Subchannel Change Summary** message does not provide an indication of the sub-channel attributes associated with the newly added sub-channel. Accordingly, the mobile will read a **Subchannel configuration message** to determine if it is interested in the new sub-channel and read a cycle of that sub-channel as desired.

As another example, consider a mobile station that is informed of a change in S-BCCH information via the S-BCCH change notification flag carried in the SPACH header. Suppose, for this example, that the change constitutes the modification of a single message sent on a specific sub-channel of interest to the mobile station. The mobile station responds to the change notification by first reading sub-channel 0 to acquire the **Sub-channel Change Summary** message. The **Change Indicator Map** information element contained within this message identifies that only a single sub-channel has changed. A bit position in the **Change Indicator Map** information element and its corresponding value serves to uniquely identify the changed sub-channel. The **Change Acquisition Map** information element, also contained within this message, indicates how the

-59-

changed information is to be acquired for the changed sub-channel identified. For this example, assume that the bit position in the **Change Acquisition Map** information element corresponding to the changed sub-channel indicates that sub-channel 1 should be read to acquire the changes associated with the changed sub-channel. The mobile station then proceeds to read a full set of information sent on sub-channel 1 (in this example only a single S-BCCH Payload message since only one sub-channel has changed) and updates its S-BCCH information accordingly.

Although the present invention has been described in terms of attributes such as types of encryption and user group assignment, those skilled in the art will appreciate that other types of attributes can be added or substituted for those described herein. Moreover, other broadcast SMS embodiments will also be apparent to those skilled in the art as being within the scope of the present invention without a detailed description thereof. For example, sub-channel 1 need not be dedicated to carry change information. Instead, additional segmentation can be provided at Layer 2 whereby strings of Layer 2 frames are also defined to allow guaranteed delivery of these distinct strings without interruption (unless aborted) while still allowing for a fast real time response to information change situations.

Another technique would be to provide only a single (large) payload sub-channel used for carrying the full set of broadcast information rather than the exemplary sub-channels 2...32 described above. Changes could still be carried on sub-channel 1 and sub-channel 0 could still contain sub-channel structure and detailed change indication information. Message encryption and user group operation would then be specified on a per BCCH message basis.

Moreover, although these illustrative embodiments describe a mobile station that first reads sub-channel 0 upon receiving a change notification, those skilled in the art will appreciate that the mobile station could vary this procedure. For example, sub-channel 1 could be read first by the mobile station to determine which messages have changed. A change flag could be provided on sub-channel

-60-

1 to indicate whether or the information on sub-channel 0 has changed, at which point the mobile station could then acquire the S-BCCH information of sub-channel 0.

5 It is, of course, possible to embody the invention in specific forms other than those described above without departing from the spirit of the invention. The embodiments described above are merely illustrative and should not be considered restrictive in any way. The scope of the invention is determined by the following claims, rather than the preceding description, and all variations and
10 equivalents which fall within the scope of the claims are intended to be embraced therein.

-61-

WHAT IS CLAIMED IS:

1. A method of communicating information to a remote station comprising the steps of:
 - grouping the information into a plurality of successive time slots on a
5 radio carrier signal;
 - grouping the time slots into a plurality of successive superframes; and
 - grouping the successive superframes into a plurality of successive hyperframes, wherein at least two successive superframes are grouped into each hyperframe;
 - 10 wherein each superframe includes time slots comprising a logical channel for broadcast control information and time slots comprising a logical paging channel, and the broadcast control information comprises special messages that are included in respective time slots comprising a logical special message channel.
- 15 2. The method of claim 1, wherein the time slots of the special message channel are grouped in successive SMS frames, and the SMS frames are synchronized with respective hyperframes.
3. The method of claim 2, wherein each SMS frame corresponds to a respective one of a plurality of SMS sub-channels.
- 20 4. The method of claim 3, wherein a special message spans at least two SMS frames of a respective SMS sub-channel.
5. The method of claim 3, wherein the special messages included in the time slots of a first one of the SMS sub-channels are encrypted according to a first encryption method and the special messages included in the time slots of at
25 least one other SMS sub-channel are encrypted according to another encryption method.
6. The method of claim 3, wherein each special message is encrypted according to a respective encryption method.

-62-

7. A method for transmitting messages in a radiocommunication system, comprising the steps of:

- identifying a plurality of attributes associated with said messages;
- selecting subsets of said attributes;
- 5 grouping said messages using said selected subsets and at least one attribute associated with each message; and
- selectively transmitting said groups of messages.

8. The method for transmitting messages of claim 8, wherein said step of identifying further comprises:

- 10 identifying a plurality of encryption techniques and a plurality of user groups as said plurality of attributes.

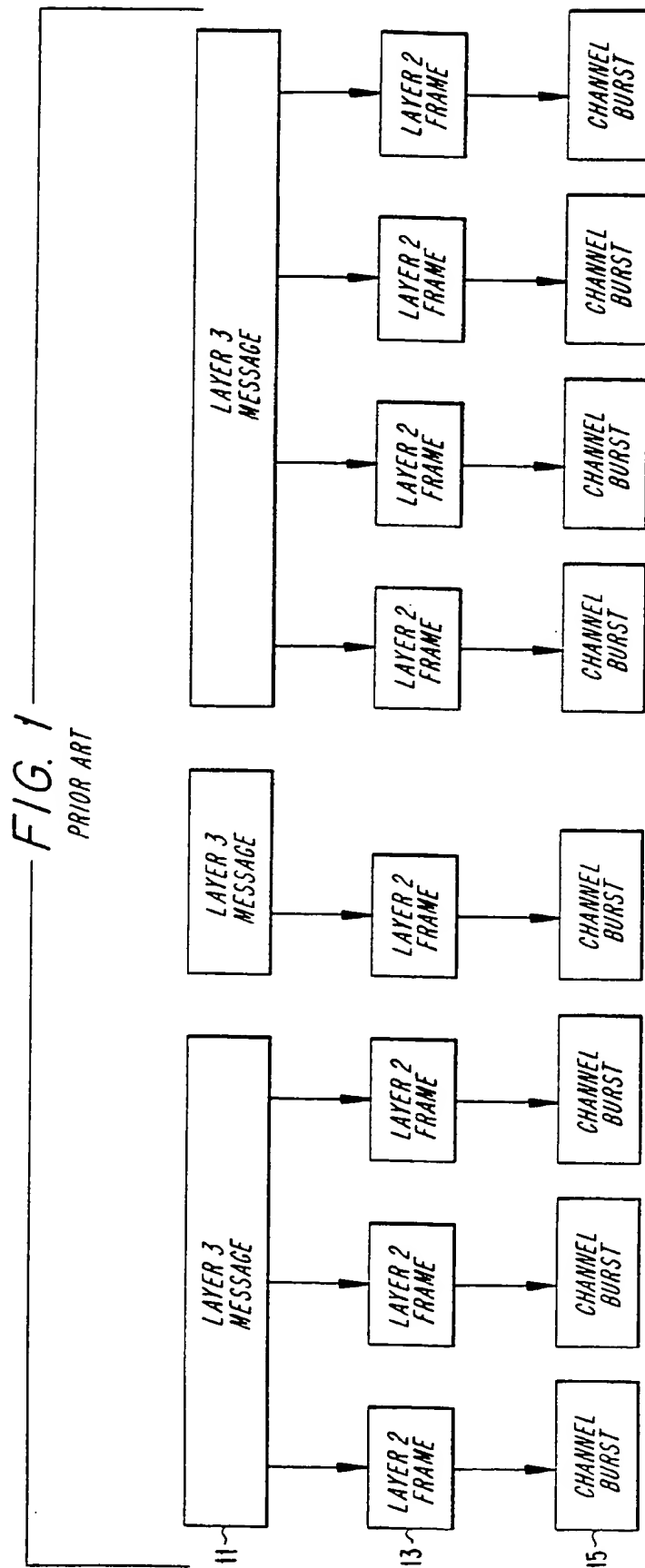
9. The method for transmitting messages of claim 8, wherein said steps of selecting subsets and grouping messages further comprise:

- 15 selecting a subset including a first one of said plurality of encryption techniques; and
- grouping together messages having as said at least one attribute said first one of said plurality of encryption techniques.

10. The method for transmitting messages of claim 8, wherein said steps of selecting subsets and grouping messages further comprise:

- 20 selecting a subset including a first one of said plurality of user groups; and
- grouping together messages having as said at least one attribute a user group identification associated with said first one of said plurality of user groups.

1/10



2/10

FIG. 2

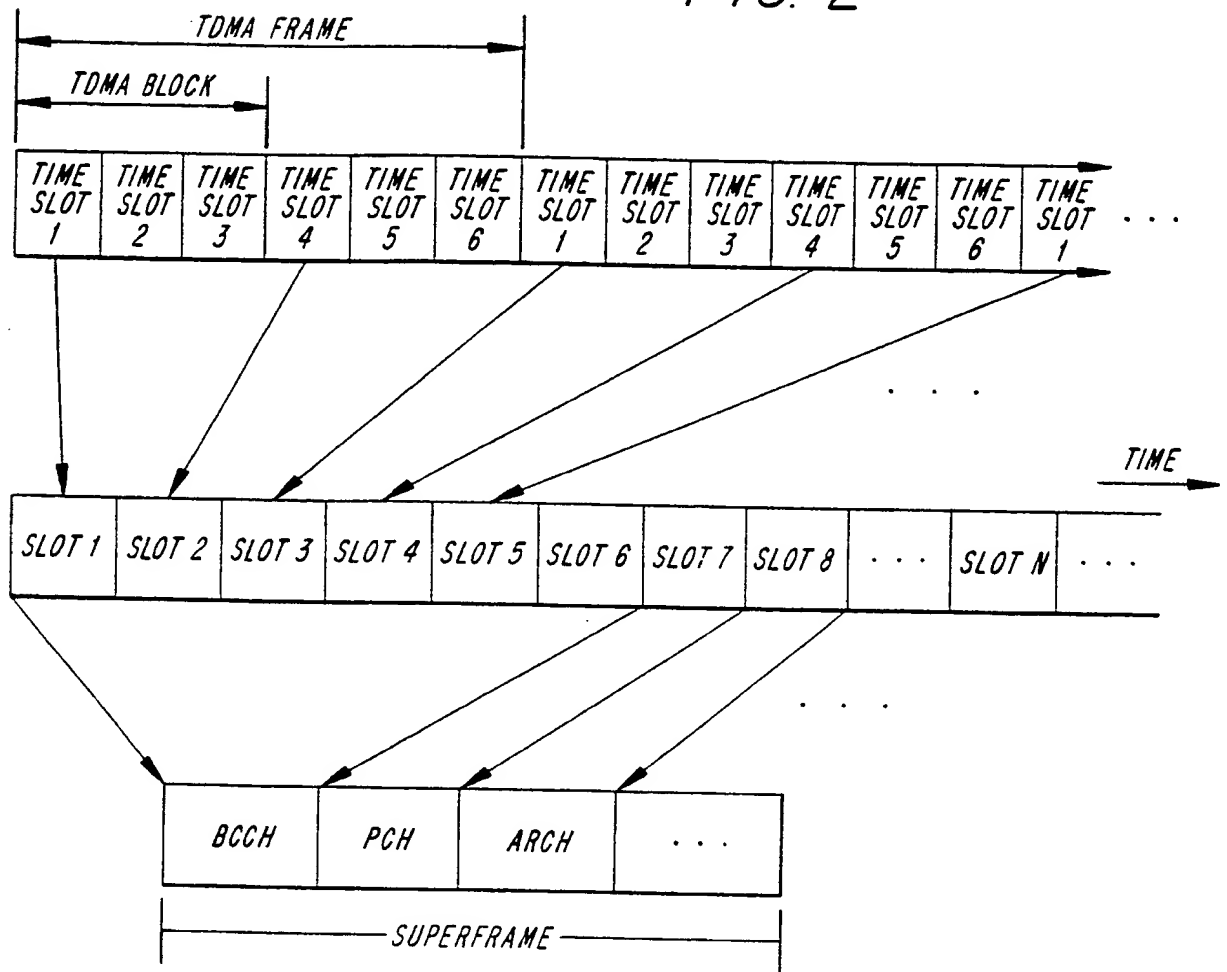
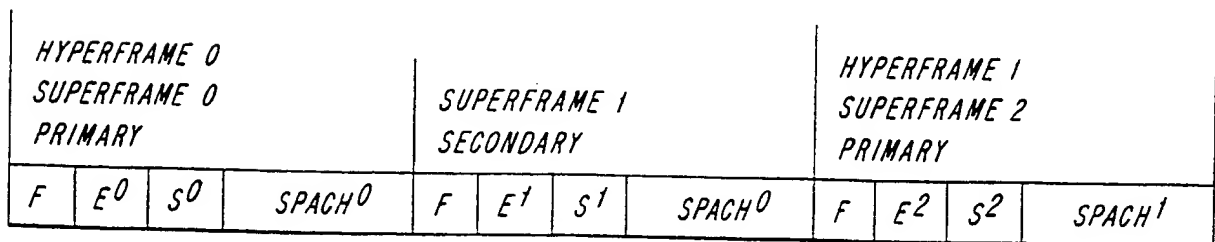


FIG. 5



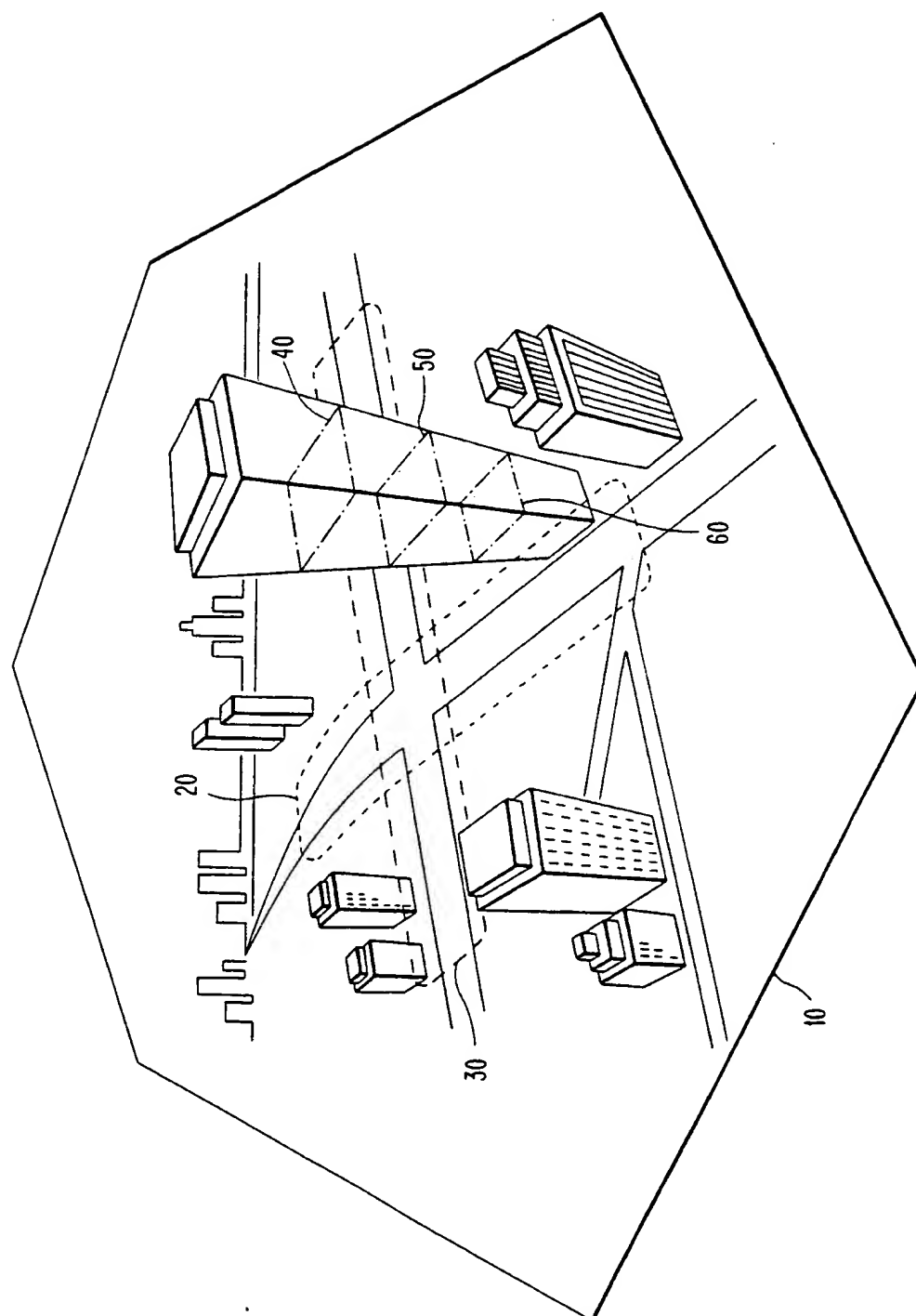
F = F-BCCH

E = E-BCCH

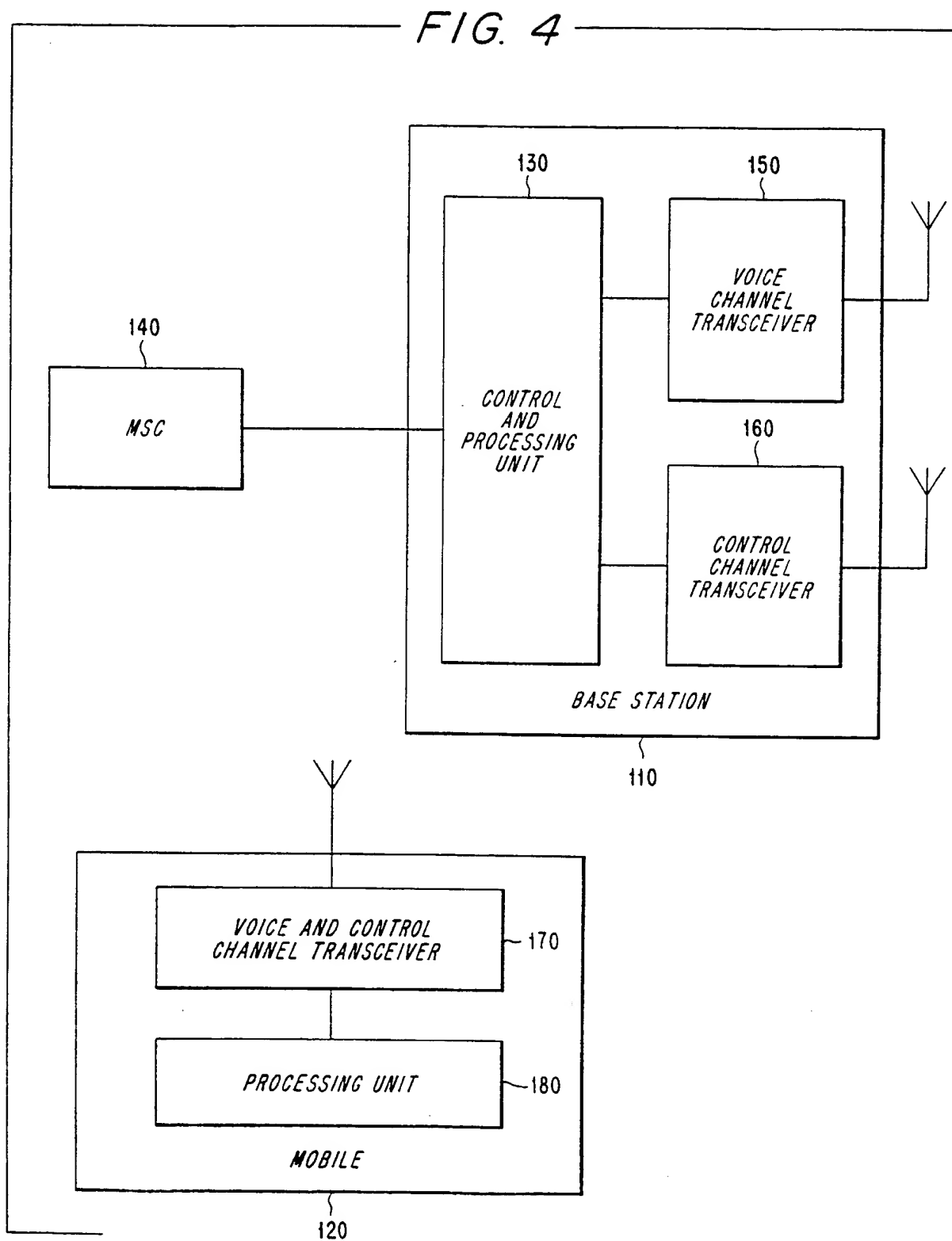
S = S-BCCH

SPACH = PCH OR ARCH OR SMSCH

FIG. 3



4/10



5/10

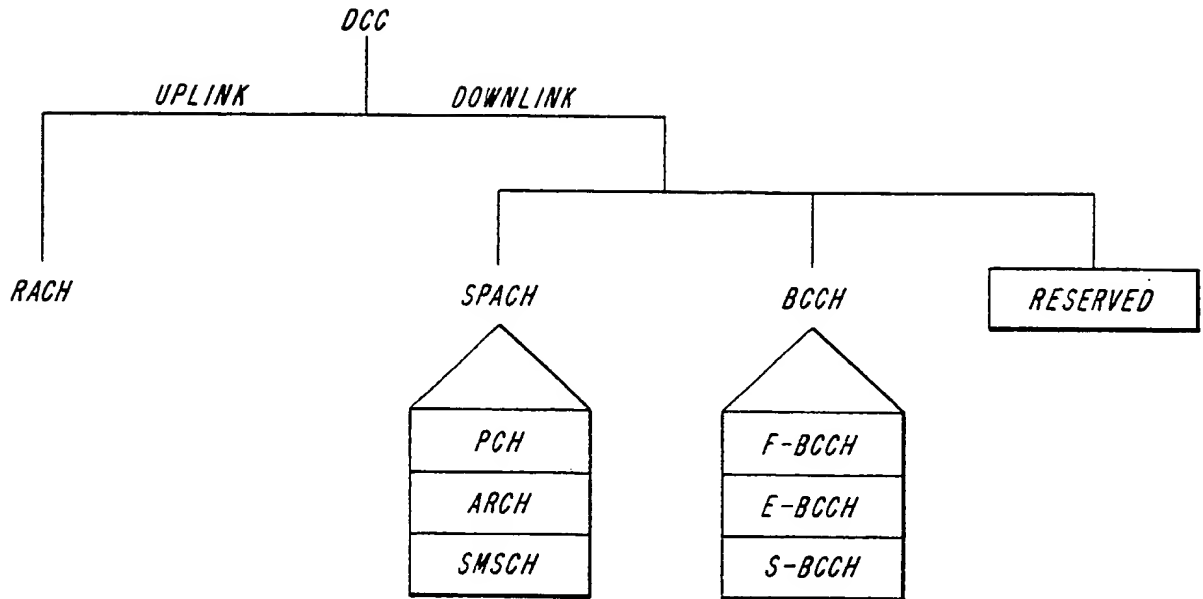


FIG. 6

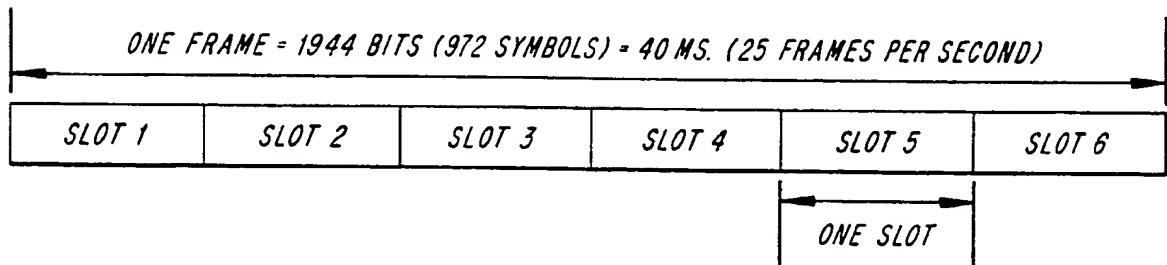


FIG. 7

6/10

FIG. 8a

6	6	16	28	122	24	122
G	R	PREAM	SYNC	DATA	SYNC+	DATA

FIG. 8b

6	6	16	28	122	24	78	44
G	R	PREAM	SYNC	DATA	SYNC+	DATA	AG

FIG. 8c

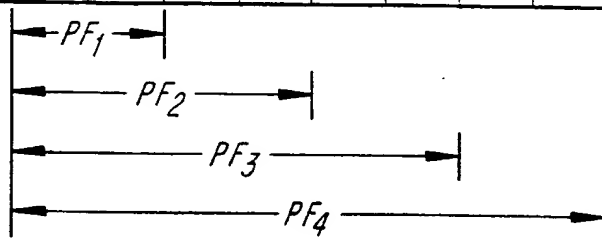
28	3	3	6	130	12	130	3	2	5	2
SYNC	BRI	R/N	CPE	DATA	CSFP	DATA	BRI	R/N	CPE	RSVD

- AG — ABBREVIATED GUARD TIME
 BRI — BUSY/RESERVED/IDLE INDICATOR
 CSFP — CODED SUPER FRAME PHASE
 DATA — INFORMATION BITS
 G — GUARD TIME
 CPE — CODED PARTIAL ECHO
 PREAM — PREAMBLE
 R — RAMP TIME
 R/N — RECEIVED/NOT RECEIVED
 RSVD — RESERVED FIELD, SET TO 11
 SYNC — SYNCHRONIZATION
 SYNC+ — ADDITIONAL SYNCHRONIZATION

7/10

FIG. 10

HF_n	0		1		2		3		4		5		6	
SF_n	0	1	2	3	4	5	6	7	8	9	10	11	12	13
PF_1	p	s	p	s	p	s	p	s	p	s	p	s	p	s
PF_2	p	s	-	-	p	s	-	-	p	s	-	-	p	s
PF_3	p	s	-	-	-	-	p	s	-	-	-	-	p	s
PF_4	p	s	-	-	-	-	-	-	p	s	-	-	-	-



HF = HYPERFRAME
 SF = SUPERFRAME
 PF = PAGING FRAME
 P = PRIMARY PCHs
 S = SECONDARY PCHs

FIG. 9

109/101/79	16	5
INFORMATION	CRC	TAIL

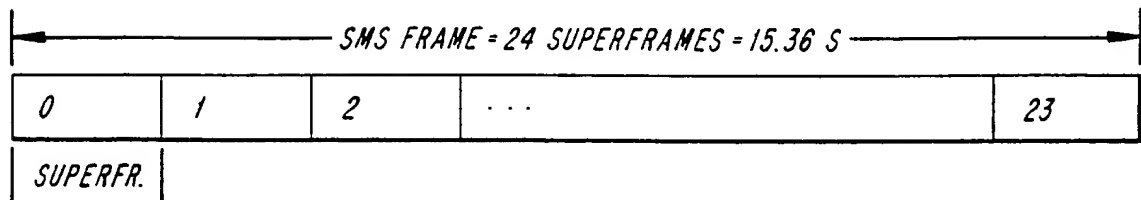


FIG. 11

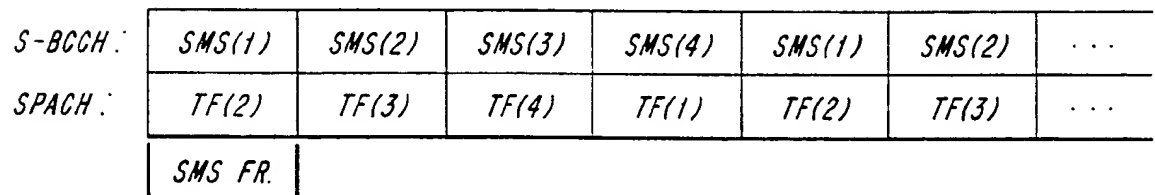


FIG. 12

FIG. 13a

SCS = X	BC = 0	L3LI = X...X	L3DATA = X...X	BE = 1	FILLER = 0...0	CRC = X...X
1	1	8	1	1		16

FIG. 13b

SCS = X	BC = 0	L3LI = X...X	L3DATA = X...X	BE = 0	L3LI = X...X	L3DATA = X...X	CRC = X...X
1	1	8	1	1	8		16

FIG. 13c

SCS = X	BC = 1	CLI = X...X	L3DATA = X...X	BE = 1	FILLER = 0...0	CRC = X...X
1	1	7	1	1		16

FIG. 14a

BC = 0	SID = 7	FDC = 4	SSI = 1	SCN = 0	L3LI = X...X	L3DATA = X...X	CRC = X...X
1	5	8	1	1	8	85	16

FIG. 14b

BC = 1	SID = 7	FDC = 1	SSI = 0	SCN = 0	CLI = X...X	L3DATA = X...X	BI = 0	FILLER = 0...0	CRC = X...X
1	5	8	1	1	7	1	1	16	

FIG. 14c

BC = 1	SID = 7	FDC = 3	SSI = 0	SCN = 0	CLI = X...X	L3DATA = X...X	BI = 1	L3LI = X...X	L3DATA = X...X	CRC = X...X
1	5	8	1	1	7	1	8	16		

FIG. 14d

BC = 1	SID = 7	FDC = 2	SSI = 0	SCN = 0	CLI = X...X	L3DATA = X...X	CRC = X...X
1	5	8	1	1	7	86	16

INTERNATIONAL SEARCH REPORT

International Application No

PCT/SE 96/00716

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04Q7/38 H04B7/24

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 H04Q H04B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	W0,A,95 12931 (ERICSSON) 11 May 1995 cited in the application see page 41, line 1 - line 25; claims 1,3,11,13,14,27,28 ---	1-10
X	W0,A,95 12936 (ERICSSON) 11 May 1995 see claims 41-52 ---	7-10
X	US,A,5 267 175 (HOOOPER) 30 November 1993 see column 3, line 18 - column 4, line 24 -----	7-10

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- *&* document member of the same patent family

Date of the actual completion of the international search

18 October 1996

Date of mailing of the international search report

12.11.96

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl,
Fax (+ 31-70) 340-3016

Authorized officer

Bischof, J-L

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/SE 96/00716

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO-A-9512931	11-05-95	AU-A- 1048095	23-05-95
		AU-A- 1048395	23-05-95
		AU-A- 1087495	23-05-95
		AU-A- 1087695	23-05-95
		AU-A- 7757094	18-05-95
		AU-A- 8131394	23-05-95
		AU-A- 8131494	23-05-95
		BR-A- 9404316	04-07-95
		BR-A- 9405702	28-11-95
		BR-A- 9405703	28-11-95
		BR-A- 9405704	28-11-95
		BR-A- 9405705	28-11-95
		BR-A- 9405743	05-12-95
		BR-A- 9405927	05-12-95
		CA-A- 2134695	02-05-95
		CA-A- 2152942	11-05-95
		CA-A- 2152943	11-05-95
		CA-A- 2152944	11-05-95
		CA-A- 2152945	11-05-95
		CA-A- 2152946	11-05-95
		CA-A- 2152947	11-05-95
		CN-A- 1112345	22-11-95
		CN-A- 1117329	21-02-96
		CN-A- 1116888	14-02-96
		CN-A- 1117330	21-02-96
		CN-A- 1117331	21-02-96
		CN-A- 1124074	05-06-96
		CN-A- 1117332	21-02-96
		EP-A- 0652680	10-05-95
		EP-A- 0682829	22-11-95
		EP-A- 0679304	02-11-95
		EP-A- 0677222	18-10-95
		EP-A- 0681766	15-11-95
		EP-A- 0677223	18-10-95
		EP-A- 0677224	18-10-95
		FI-A- 953262	30-08-95
		FI-A- 953263	30-06-95
		FI-A- 953264	30-06-95
		FI-A- 953265	30-06-95
		FI-A- 953266	30-06-95

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/SE 96/00716

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO-A-9512931		FI-A- 953267	22-08-95
		FI-A- 953268	30-06-95
		JP-T- 8508627	10-09-96
		JP-T- 8508628	10-09-96
		JP-T- 8508629	10-09-96
		JP-T- 8508630	10-09-96
		JP-T- 8508631	10-09-96
		SE-A- 9403725	19-06-95
		WO-A- 9512933	11-05-95
		WO-A- 9512934	11-05-95

WO-A-9512936	11-05-95	AU-A- 1048095	23-05-95
		AU-A- 1048395	23-05-95
		AU-A- 1087495	23-05-95
		AU-A- 1087695	23-05-95
		AU-A- 7757094	18-05-95
		AU-A- 8131394	23-05-95
		AU-A- 8131494	23-05-95
		BR-A- 9404316	04-07-95
		BR-A- 9405702	28-11-95
		BR-A- 9405703	28-11-95
		BR-A- 9405704	28-11-95
		BR-A- 9405705	28-11-95
		BR-A- 9405743	05-12-95
		BR-A- 9405927	05-12-95
		CA-A- 2134695	02-05-95
		CA-A- 2152942	11-05-95
		CA-A- 2152943	11-05-95
		CA-A- 2152944	11-05-95
		CA-A- 2152945	11-05-95
		CA-A- 2152946	11-05-95
		CA-A- 2152947	11-05-95
		CN-A- 1112345	22-11-95
		CN-A- 1117329	21-02-96
		CN-A- 1116888	14-02-96
		CN-A- 1117330	21-02-96
		CN-A- 1117331	21-02-96
		CN-A- 1124074	05-06-96
		CN-A- 1117332	21-02-96
		EP-A- 0652680	10-05-95

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/SE 96/00716

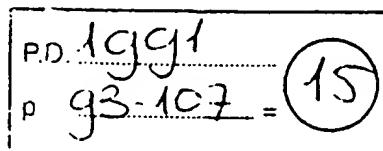
Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO-A-9512936		EP-A- 0682829	22-11-95
		EP-A- 0679304	02-11-95
		EP-A- 0677222	18-10-95
		EP-A- 0681766	15-11-95
		EP-A- 0677223	18-10-95
		EP-A- 0677224	18-10-95
		FI-A- 953262	30-08-95
		FI-A- 953263	30-06-95
		FI-A- 953264	30-06-95
		FI-A- 953265	30-06-95
		FI-A- 953266	30-06-95
		FI-A- 953267	22-08-95
		FI-A- 953268	30-06-95
		JP-T- 8508627	10-09-96
		JP-T- 8508628	10-09-96
		JP-T- 8508629	10-09-96
		JP-T- 8508630	10-09-96
		JP-T- 8508631	10-09-96
		SE-A- 9403725	19-06-95
		WO-A- 9512933	11-05-95
		WO-A- 9512934	11-05-95
US-A-5267175	30-11-93	AU-A- 7728287	17-03-88
		EP-A- 0267379	18-05-88
		JP-A- 63153675	27-06-88

XP 000472724

Smart Card 2000
D. Chaum (Editor)
© 1991 Elsevier Science Publishers B.V. All rights reserved

0000-328
70400:1252

93-107



Smart Card Technology Applied to the future European Cellular Telephone on the digital D-Network

A.J. Farrugia^a and P. Peyret^b

^a ^bGEMPLUS CARD International, Avenue du Pic de Bertagne, Parc d'activités de la plaine de Jouques. PO Box 100 13881 GEMENOS Cedex.

I. ABOUT THIS DOCUMENT

This document is an overview of the application of smart card technology as used in the Subscriber Identity Modules of the future European mobile cellular telephone system based on the digital D-network.

It is not an official document and, as such, does not involve the responsibility of official bodies whatsoever.

This document is the property of GEMPLUS Card International. It must not be copied partly or in full without obtaining the prior written consent of GEMPLUS.

II. BACKGROUND

The task of specifying and standardizing a cellular mobile-phone system using digital RF transmission within the 900-MHz band has been undertaken in Europe in the early eighties. Since then, the work done by the CEPT¹, which was later to become the ETSI², has covered the description of potential services, as well as the functions of the system, the interfaces between the system components, including the RF characteristics, and has led to a coherent set of technical recommendations.

Because the working group was known as the "Groupe Spécial Mobiles", such systems as described in the set of recommendations are designated as GSM systems.

The GSM recommendations make use of advanced technologies in many aspects of the system:

- full-digital RF transmission with low bit-rate coding
- ISDN-type layered protocols in the networks
- CCITT N°7 protocol handling between networks

¹ CEPT = Conference Européenne des postes et telecommunications

² European Telecommunications Standards Institute

THIS PAGE BLANK (USPTO)

1. Public Land Mobile Network (PLMN)

The PLMN designates an homogeneous part of the cellular phone network operated by one entity such as an Operator (or Consortium of Operators).

For example, a subscriber will have a Home PLMN, covering the geographical area of his main residence, the operator of which he is likely to get his subscription from. When travelling abroad, he may access services through other PLMNs.

2. Mobile Station (MS)

The MS is the functional element which allows the subscriber to access the telecommunication services.

Depending on the type of services it provides access to (e.g. vocal only or vocal + non-vocal), and depending on the characteristics of its RF part (such as range), a Mobile Station can be of one of three types:

- "car" station: to be installed in a vehicle
- "portable" station: can be moved around when necessary
- "pocket" or "hand-held" station: small enough to be carried around at all times

3. Mobile Equipment (ME)

The part of the Mobile Station excluding the Subscriber Identity Module

4. Subscriber Identity Module (SIM)

The removable part of the MS which contains the information related to the Subscriber. It is physically and logically distinct from the rest of the station.

Two physical implementations can exist:

- "Card" SIM, which has the same dimensions as a credit card and complies to the ISO IS 7816-1, -2 for the physical layout.
- "Plug-In" SIM which is smaller than a credit card, hence is best suited for portable and pocket stations. The Plug-In SIM is installed semi-

THIS PAGE BLANK (USPTO)

10. Location Area Identification (LAI)

The Location Area Identification is the data which identify to the network where the mobile subscriber is currently located. The LAI and the TMSI are maintained in both the Mobile Station and the Location Registers (see below).

11. Home Location Register (HLR)

Register where the references to the subscriber having subscribed locally are maintained. The HLR is in fact a (piece of a) data base in a specialized computer.

12. Visitor Location Register (VLR)

Register where the references to "roaming" subscribers considered currently as visitors are maintained. The VLR is in fact a (piece of a) data base in a specialized computer.

13. Key for Authentication (Ki)

The Subscriber Authentication key Ki is a fixed, secret and personal key which is used to authenticate the subscriber upon accessing the network. Ki is used to compute the Signed Response (see below) and the Cipherring Key (see below)

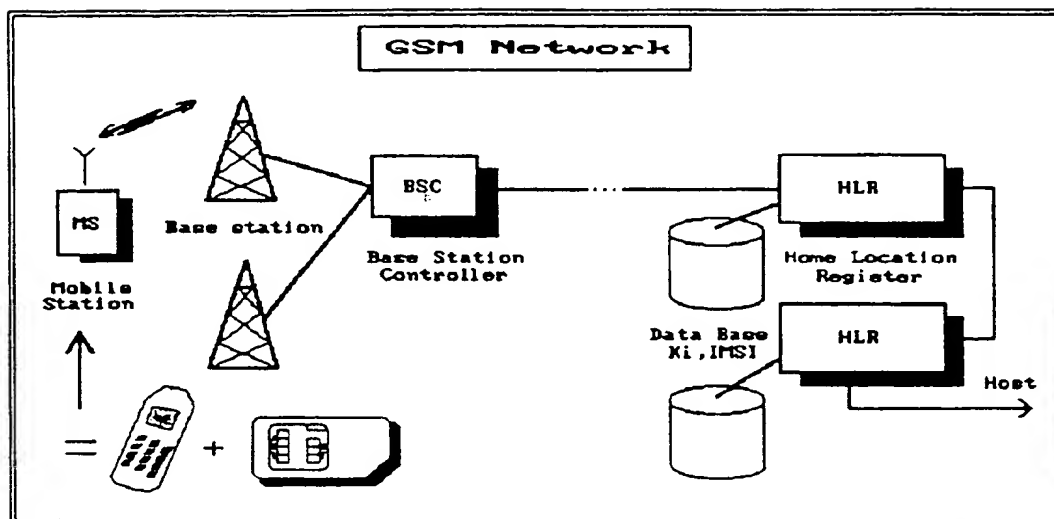
14. Key for Cipherring (Kc)

The Cipherring Key Kc is used to cipher/decipher the data transmitted over the RF channel, thus providing confidentiality of the transmission. Kc is only valid for one session, i.e. from one authentication until the next one.

15. Signed Response (SRES)

The Signed Response is a signature number computed by the authentication algorithm A3 (see below), using a random number and the key Ki as inputs. The SRES is computed in the SIM of the Mobile Station, and sent back to the originator of the random number for comparison with a value computed locally.

THIS PAGE BLANK (USPTO)



C. Services

Potential services offered to the subscribers include:

- Telephone calls (voice): make and receive
 - Emergency calls
 - Transmission of short alphanumeric messages
 - Group 3 facsimile transmission
 - Connection to packet-switched networks such as X25
- Additional features can be:

- Abbreviated dialing numbers
- Fixed dialing numbers
- Collecting charging information
- Barring of outgoing calls

It should be noted that a subscriber is always identified in the same way, whatever his geographical location at any point in time. This means that a "fixed" number can be used to reach a travelling person. This opens the doors to much more efficient business telecommunications.

Also, thanks to the basic bit-rate of 270.83 Kb/s, many tele-informatics applications will be possible.

THIS PAGE BLANK (USPTO)

1. Basic storage functions

The Subscriber is identified uniquely in the set of GSM PLMNs by its International Mobile Subscriber Identity number. This number needs to be stored securely within the SIM so that the Subscriber can be recognized unambiguously at whatever station he may use. The IMSI is a fixed number.

A Mobile Station can only be operated if there is a valid IMSI in the SIM, except for emergency calls.

Next to the IMSI, the SIM stores the TMSI (Temporary Mobile Subscriber Identity), which is the code most often used to address the Subscriber: the TMSI is only valid locally, and for a short period of time. It is used in place of the IMSI so as to maintain the identity of the Subscriber confidential.

In order to preserve the correspondence between the IMSI and the TMSI, the Location Area Identity number is needed. Like the TMSI, the LAI is not a fixed piece of data and may be replaced when re-localizing a customer.

Associated to the IMSI, is the Key for Authentication K_i , which is used as an input to the authentication algorithm. K_i is fixed and stored in a secure location.

The SIM also stores temporarily the Key for Ciphering K_c , after having computed it with the A3 algorithm (see paragraph Security functions), and before passing it to the ME. Cipher Keys are indexed with a sequence number, which is also stored in the SIM.

The SIM stores the current value of the PIN code, which it is responsible for checking (see paragraph security functions)

The SIM stores the time value related to the periodic location updating. This value is called TMSI time.

In addition, the SIM must maintain some data associated with the "house-keeping" functions such as:

- PIN error counter
- personal unblocking key
- any secret code related to administration procedures

2. Optional storage functions

The SIM may provide facilities to store and manage additional information related to the mobile subscriber in association with the GSM services:

THIS PAGE BLANK (USPTO)

The Operator may offer the possibility for the Subscriber to disable the PIN code function of the SIM. When this capability is not offered, then the user is forced to always enter his PIN code when using a MS with his SIM.

2. Authentication of the SIM to the Network

The GSM network needs to make sure that a MS requesting services corresponds to a genuine Subscriber, before that Subscriber is given access to those services and is charged for them.

The network sends a random challenge RAND, in the form of a 128 bit number, to the SIM. The SIM executes algorithm A3 internally, using RAND and Ki as inputs, and produces SRES. This signature is checked by the network with a similar algorithm; if the signature is recognized as valid, then the authentication is successful.

3. Ciphering of the transmission data

The SIM is not responsible for executing the Ciphering Algorithm A5, which resides in the ME; however, it is responsible for the computation of the Kc key used by A5.

In parallel with A3, the SIM contains the algorithm A8, which uses RAND and Ki as inputs, and produces Kc. Kc is also computed by the fixed part of the network, and is then used for the ciphering/deciphering of the following data transmissions.

V. THE SIM IMPLEMENTATION

Because of the requirements assessed above that the SIM should:

- be detachable
- provide secure storage
- execute algorithms
- be updatable
- exist in two form-factors

the SIM implementation is based on advanced Smart Card technology involving several enhanced features in the field of:

- memory and chip technology
- physical layout and characteristics
- logical memory organization and management

THIS PAGE BLANK (JBPTO)

Because a Plug-In SIM is significantly smaller than a credit card, it is not as handy and is intended to be semi-permanently installed in the station. It is up to the manufacturers of MEs to make it more or less easy to install and remove a Plug-In SIM.

Thanks to its unique manufacturing techniques based on molding, GEMPLUS is able to manufacture both Card SIMs and Plug-In SIMs very cost-efficiently.

C. SIM-ME communication protocols

As usual, two levels are distinguished to describe the communication protocol:

- the transmission protocol
- the application protocol

1. Transmission protocol

Regardless of whether the SIM is a Card or a Plug-In module, the transmission protocol conforms to the ISO IS7816-3 standard, using the character mode "T=0".

Although some newer protocols are currently under discussion in the ISO, it was necessary to agree on existing standards in order to match the 1991 deadline. The transmission protocol chosen is quite well adapted to the SIM application.

2. Application protocol

Messages exchanged between the SIM and the ME (or between the SIM and an accepting device during the administrative phase) are divided into:

- Commands (sent to the SIM)
- Responses (received from the SIM)

A GSM instruction is made up of a Command-Response pair, where a response is associated to one command. The response contains condition codes that may be accompanied by data.

A GSM procedure is a sequence of instructions which is supposed to be executed without interruption. Examples of procedures can be:

- User PIN code verification
- IMSI request
- short message erasure

THIS PAGE BLANK (USPTO)

4. Actions on data-fields and directories

Actions that can be performed on data-fields, when in GSM mode include:

- selection
- update the contents
- read the contents
- seek (in the case of formatted data-fields)

The only action allowed on Directories in GSM mode is:

E. Security Policies

The definition of the rules allowing a specific party to access and perform specific actions on data stored in the SIM is called a security policy.

A security policy is attached to each data-field, which is the smallest entity which can be protected by an individual policy. The various actions that can be performed on a data-field must meet the access conditions specified in the security policy of the target data-field.

Also, a security policy of a higher level may be attached to the Directories. When this is the case, then both the security policy of the directory and the security policy of the data-fields belonging to that directory must be respected in order to perform any action.

The security policy for directories and for the data-fields have the same structure and include conditions for six actions:

- Read or Seek
- Update

Each condition is handled independently and can take the following values:

- ALWAYS possible (no checking)
- PIN: allowed if PIN code checked or PIN function disabled
- ADM: allowed if an authentication procedure used at the administrative phase has been successful
- NEVER possible

THIS PAGE BLANK (USPTO)

PCTWORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : H04Q 7/38, H04B 7/24	A1	(11) International Publication Number: WO 96/41493 (43) International Publication Date: 19 December 1996 (19.12.96)
(21) International Application Number: PCT/SE96/00716 (22) International Filing Date: 31 May 1996 (31.05.96) (30) Priority Data: 08/482,754 7 June 1995 (07.06.95) US (71) Applicant: TELEFONAKTIEBOLAGET LM ERICSSON (publ) [SE/SE]; S-126 25 Stockholm (SE). (72) Inventors: DIACHINA, John, W.; 505 Kristin Drive, Garner, NC 27529 (US). RAITH, Alex, K.; Park Ridge Road 805- A5, Durham, NC 27713 (US). PERSSON, Bengt; P.O. Box 42, S-182 05 Djurshamn (SE). SAMMARCO, Anthony, J.; 605 Benfield Court, Garner, NC 27529 (US). (74) Agents: BOHLIN, Björn et al.; Telefonaktiebolaget LM Eric- sson, Patent and Trademark Dept., S-126 25 Stockholm (SE).		(81) Designated States: AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG). Published <i>With international search report.</i> <i>Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i>
(54) Title: DIGITAL CONTROL CHANNELS HAVING LOGICAL CHANNELS SUPPORTING BROADCAST SMS		
(57) Abstract A communications system in which information is transmitted in successive time slots grouped into a plurality of superframes which are, in turn, grouped into a plurality of hyperframes. A remote station is assigned to one of the time slots in each of the superframes for paging the remote station, each hyperframe including at least two superframes, and the information sent in the assigned time slot in one superframe in each hyperframe is repeated in the assigned time slot in the other superframe(s) in each hyperframe. Each superframe can include a plurality of time slots used for sending paging messages to remote stations, grouped into a plurality of successive paging frames, and the time slot to which the remote station is assigned is included once in every paging frame. Also, each superframe may include time slots comprising a logical channel for broadcast control information and time slots comprising a logical paging channel. Information sent in the assigned time slot may direct the remote station to read the broadcast control information, and the information may have been encoded according to an error correcting code and include a plurality of bits having polarities that are inverses of cyclic redundancy check bits produced by the encoding. Also, the broadcast control information may comprise special messages that are included in respective time slots comprising a logical special message channel, the time slots of the special message channel may be grouped in successive SMS frames, and the SMS frames may be synchronized to start with a start of a superframe.		

THIS PAGE BLANK (USPTO)

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	GB	United Kingdom	MW	Malawi
AT	Austria	GE	Georgia	MX	Mexico
AU	Australia	GN	Guinea	NE	Niger
BB	Barbados	GR	Greece	NL	Netherlands
BE	Belgium	HU	Hungary	NO	Norway
BF	Burkina Faso	IE	Ireland	NZ	New Zealand
BG	Bulgaria	IT	Italy	PL	Poland
BJ	Benin	JP	Japan	PT	Portugal
BR	Brazil	KE	Kenya	RO	Romania
BY	Belarus	KG	Kyrgyzstan	RU	Russian Federation
CA	Canada	KP	Democratic People's Republic of Korea	SD	Sudan
CF	Central African Republic	KR	Republic of Korea	SE	Sweden
CG	Congo	KZ	Kazakhstan	SG	Singapore
CH	Switzerland	LI	Liechtenstein	SI	Slovenia
CI	Côte d'Ivoire	LK	Sri Lanka	SK	Slovakia
CM	Cameroon	LR	Liberia	SN	Senegal
CN	China	LT	Lithuania	SZ	Swaziland
CS	Czechoslovakia	LU	Luxembourg	TD	Chad
CZ	Czech Republic	LV	Latvia	TG	Togo
DE	Germany	MC	Monaco	TJ	Tajikistan
DK	Denmark	MD	Republic of Moldova	TT	Trinidad and Tobago
EE	Estonia	MG	Madagascar	UA	Ukraine
ES	Spain	ML	Mali	UG	Uganda
FI	Finland	MN	Mongolia	US	United States of America
FR	France	MR	Mauritania	UZ	Uzbekistan
GA	Gabon			VN	Viet Nam

THIS PAGE BLANK (USPTO)

-1-

DIGITAL CONTROL CHANNELS HAVING LOGICAL CHANNELS SUPPORTING BROADCAST SMS

This application is a continuation-in-part of U.S. Patent Application No. 08/331,703 entitled "Digital Control Channels Having Logical Channels for
5 Multiple Access Radiocommunication", which was filed on October 31, 1994 and which is incorporated in this application by reference. This parent application is a continuation in part of U.S. Patent Application No. 08/147,254 entitled "A Method for Communicating in a Wireless Communication System", which was
10 reference. The parent application is also a continuation in part of U.S. Patent Application No. 07/956,640 entitled "Digital Control Channel", which was filed on October 5, 1992, and which is incorporated in this application by reference.

BACKGROUND

Applicants' invention relates generally to radiocommunication systems
15 that use digital control channels in a multiple access scheme and more particularly to cellular TDMA radiotelephone systems having digital control channels.

The growth of commercial radiocommunications and, in particular, the explosive growth of cellular radiotelephone systems have compelled system
20 designers to search for ways to increase system capacity without reducing communication quality beyond consumer tolerance thresholds. One way to increase capacity is to use digital communication and multiple access techniques such as TDMA, in which several users are assigned respective time slots on a single radio carrier frequency.

25 In North America, these features are currently provided by a digital cellular radiotelephone system called the digital advanced mobile phone service (D-AMPS), some of the characteristics of which are specified in the interim standard IS-54B, "Dual-Mode Mobile Station-Base Station Compatibility

THIS PAGE BLANK (USPTO)

-2-

Standard", published by the Electronic Industries Association and Telecommunications Industry Association (EIA/TIA). Because of a large existing consumer base of equipment operating only in the analog domain with frequency-division multiple access (FDMA), IS-54B is a dual-mode (analog and digital) standard, providing for analog compatibility in tandem with digital communication capability. For example, the IS-54B standard provides for both FDMA analog voice channels (AVC) and TDMA digital traffic channels (DTC), and the system operator can dynamically replace one type with the other to accommodate fluctuating traffic patterns among analog and digital users. The AVCs and DTCs are implemented by frequency modulating radio carrier signals, which have frequencies near 800 megahertz (MHz) such that each radio channel has a spectral width of 30 kilohertz (KHz).

In a TDMA cellular radiotelephone system, each radio channel is divided into a series of time slots, each of which contains a burst of information from a data source, e.g., a digitally encoded portion of a voice conversation. The time slots are grouped into successive TDMA frames having a predetermined duration. The number of time slots in each TDMA frame is related to the number of different users that can simultaneously share the radio channel. If each slot in a TDMA frame is assigned to a different user, the duration of a TDMA frame is the minimum amount of time between successive time slots assigned to the same user.

The successive time slots assigned to the same user, which are usually not consecutive time slots on the radio carrier, constitute the user's digital traffic channel, which may be considered a logical channel assigned to the user. As described in more detail below, digital control channels (DCCHs) can also be provided for communicating control signals, and such a DCCH is a logical channel formed by a succession of usually non-consecutive time slots on the radio carrier.

According to IS-54B, each TDMA frame consists of six consecutive time slots and has a duration of 40 milliseconds (msec). Thus, each radio channel can

THIS PAGE BLANK (USPTO)

-3-

carry from three to six DTCs (e.g., three to six telephone conversations), depending on the source rates of the speech coder/decoders (codecs) used to digitally encode the conversations. Such speech codecs can operate at either full-rate or half-rate, with full-rate codecs being expected to be used until half-rate
5 codecs that produce acceptable speech quality are developed. A full-rate DTC requires twice as many time slots in a given time period as a half-rate DTC, and in IS-54B, each radio channel can carry up to three full-rate DTCs or up to six half-rate DTCs. Each full-rate DTC uses two slots of each TDMA frame, i.e., the first and fourth, second and fifth, or third and sixth of a TDMA frame's six
10 slots. Each half-rate DTC uses one time slot of each TDMA frame. During each DTC time slot, 324 bits are transmitted, of which the major portion, 260 bits, is due to the speech output of the codec, including bits due to error correction coding of the speech output, and the remaining bits are used for guard times and overhead signalling for purposes such as synchronization.

15 It can be seen that the TDMA cellular system operates in a buffer-and-burst, or discontinuous-transmission, mode: each mobile station transmits (and receives) only during its assigned time slots. At full rate, for example, a mobile station might transmit during slot 1, receive during slot 2, idle during slot 3, transmit during slot 4, receive during slot 5, and idle during slot 6, and then
20 repeat the cycle during succeeding TDMA frames. Therefore, the mobile station, which may be battery-powered, can be switched off, or sleep, to save power during the time slots when it is neither transmitting nor receiving. In the IS-54B system in which the mobile does not transmit and receive simultaneously, a mobile can sleep for periods of at most about 27 msec (four slots) for a half-
25 rate DTC and about 7 msec (one slot) for a full-rate DTC.

In addition to voice or traffic channels, cellular radiocommunication systems also provide paging/access, or control, channels for carrying call-setup messages between base stations and mobile stations. According to IS-54B, for example, there are twenty-one dedicated analog control channels (ACCs), which
30 have predetermined fixed frequencies for transmission and reception located near

THIS PAGE BLANK (USPTO)

-4-

800 MHz. Since these ACCs are always found at the same frequencies, they can be readily located and monitored by the mobile stations.

For example, when in an idle state (i.e., switched on but not making or receiving a call), a mobile station in an IS-54B system tunes to and then
5 regularly monitors the strongest control channel (generally, the control channel of the cell in which the mobile station is located at that moment) and may receive or initiate a call through the corresponding base station. When moving between cells while in the idle state, the mobile station will eventually "lose" radio connection on the control channel of the "old" cell and tune to the control
10 channel of the "new" cell. The initial tuning and subsequent re-tuning to control channels are both accomplished automatically by scanning all the available control channels at their known frequencies to find the "best" control channel. When a control channel with good reception quality is found, the mobile station remains tuned to this channel until the quality deteriorates again. In this way,
15 mobile stations stay "in touch" with the system. The ACCs specified in IS-54B require the mobile stations to remain continuously "awake" (or at least for a significant part of the time, e.g. 50%) in the idle state, at least to the extent that they must keep their receivers switched on.

While in the idle state, a mobile station must monitor the control channel
20 for paging messages addressed to it. For example, when an ordinary telephone (land-line) subscriber calls a mobile subscriber, the call is directed from the public switched telephone network (PSTN) to a mobile switching center (MSC) that analyzes the dialed number. If the dialed number is validated, the MSC requests some or all of a number of radio base stations to page the called mobile
25 station by transmitting over their respective control channels paging messages that contain the mobile identification number (MIN) of the called mobile station. Each idle mobile station receiving a paging message compares the received MIN with its own stored MIN. The mobile station with the matching stored MIN transmits a page response over the particular control channel to the base station,
30 which forwards the page response to the MSC.

THIS PAGE BLANK (USPTO)

-5-

Upon receiving the page response, the MSC selects an AVC or a DTC available to the base station that received the page response, switches on a corresponding radio transceiver in that base station, and causes that base station to send a message via the control channel to the called mobile station that
5 instructs the called mobile station to tune to the selected voice or traffic channel. A through-connection for the call is established once the mobile station has tuned to the selected AVC or DTC.

When a mobile subscriber initiates a call, e.g., by dialing the telephone number of an ordinary subscriber and pressing the "send" button on the mobile
10 station, the mobile station transmits the dialed number and its MIN and an electronic serial number (ESN) over the control channel to the base station. The ESN is a factory-set, "unchangeable" number designed to protect against the unauthorized use of the mobile station. The base station forwards the received numbers to the MSC, which validates the mobile station, selects an AVC or
15 DTC, and establishes a through-connection for the call as described above. The mobile may also be required to send an authentication message.

It will be understood that a communication system that uses ACCs has a number of deficiencies. For example, the format of the forward analog control channel specified in IS-54B is largely inflexible and not conducive to the
20 objectives of modern cellular telephony, including the extension of mobile station battery life. In particular, the time interval between transmission of certain broadcast messages is fixed and the order in which messages are handled is also rigid. Also, mobile stations are required to re-read messages that may not have changed, wasting battery power. These deficiencies can be remedied by
25 providing a DCCH having new formats and processes, one example of which is described in U.S. Patent Application No. 07/956,640 entitled "Digital Control Channel", which was filed on October 5, 1992, and which is incorporated in this application by reference. Using such DCCHs, each IS-54B radio channel can carry DTCs only, DCCHs only, or a mixture of both DTCs and DCCHs.
30 Within the IS-54B framework, each radio carrier frequency can have up to three

THIS PAGE BLANK (0000)

-6-

full-rate DTCs/DCCHs, or six half-rate DTCs/DCCHs, or any combination in-between, for example, one full-rate and four half-rate DTCs/DCCHs. As described in this application, a DCCH in accordance with Applicants' invention provides a further increase in functionality.

5 In general, however, the transmission rate of the DCCH need not coincide with the half-rate and full-rate specified in IS-54B, and the length of the DCCH slots may not be uniform and may not coincide with the length of the DTC slots. The DCCH may be defined on an IS-54B radio channel and may consist, for example, of every n-th slot in the stream of consecutive TDMA slots. In this case, the length of each DCCH slot may or may not be equal to 6.67 msec, 10 which is the length of a DTC slot according to IS-54B. Alternatively (and without limitation on other possible alternatives), these DCCH slots may be defined in other ways known to one skilled in the art.

As such hybrid analog/digital systems mature, the number of analog users 15 should diminish and the number of digital users should increase until all of the analog voice and control channels are replaced by digital traffic and control channels. When that occurs, the current dual-mode mobile terminals can be replaced by less expensive digital-only mobile units, which would be unable to scan the ACCs currently provided in the IS-54B system. One conventional 20 radiocommunication system used in Europe, known as GSM, is already an all-digital system, in which 200-KHz-wide radio channels are located near 900 MHz. Each GSM radio channel has a gross data rate of 270 kilobits per second and is divided into eight full-rate traffic channels (each traffic time slot carrying 116 encrypted bits).

25 In cellular telephone systems, an air-interface communications link protocol is required in order to allow a mobile station to communicate with the base stations and MSC. The communications link protocol is used to initiate and to receive cellular telephone calls. As described in U.S. Patent Application No. 08/047,452 entitled "Layer 2 Protocol for the Random Access Channel and 30 the Access Response Channel," which was filed on April 19, 1993, and which is

THIS PAGE BLANK (USPTO)

-7-

incorporated in this application by reference, the communications link protocol is commonly referred to within the communications industry as a Layer 2 protocol, and its functionality includes the delimiting, or framing, of Layer 3 messages. These Layer 3 messages may be sent between communicating Layer 3 peer entities residing within mobile stations and cellular switching systems. The physical layer (Layer 1) defines the parameters of the physical communications channel, e.g., radio frequency spacing, modulation characteristics, etc. Layer 2 defines the techniques necessary for the accurate transmission of information within the constraints of the physical channel, e.g., error correction and detection, etc. Layer 3 defines the procedures for reception and processing of information transmitted over the physical channel.

Communications between mobile stations and the cellular switching system (the base stations and the MSC) can be described in general with reference to FIGS. 1 and 2. FIG. 1 schematically illustrates pluralities of Layer 3 messages 11, Layer 2 frames 13, and Layer 1 channel bursts, or time slots, 15. In FIG. 1, each group of channel bursts corresponding to each Layer 3 message may constitute a logical channel, and as described above, the channel bursts for a given Layer 3 message would usually not be consecutive slots on an IS-54B carrier. On the other hand, the channel bursts could be consecutive; as soon as one time slot ends, the next time slot could begin.

Each Layer 1 channel burst 15 contains a complete Layer 2 frame as well as other information such as, for example, error correction information and other overhead information used for Layer 1 operation. Each Layer 2 frame contains at least a portion of a Layer 3 message as well as overhead information used for Layer 2 operation. Although not indicated in FIG. 1, each Layer 3 message would include various information elements that can be considered the payload of the message, a header portion for identifying the respective message's type, and possibly padding.

Each Layer 1 burst and each Layer 2 frame is divided into a plurality of different fields. In particular, a limited-length DATA field in each Layer 2

THIS PAGE BLANK (USPTO)

-8-

frame contains the Layer 3 message 11. Since Layer 3 messages have variable lengths depending upon the amount of information contained in the Layer 3 message, a plurality of Layer 2 frames may be needed for transmission of a single Layer 3 message. As a result, a plurality of Layer 1 channel bursts may also be needed to transmit the entire Layer 3 message as there is a one-to-one correspondence between channel bursts and Layer 2 frames.

As noted above, when more than one channel burst is required to send a Layer 3 message, the several bursts are not usually consecutive bursts on the radio channel. Moreover, the several bursts are not even usually successive bursts devoted to the particular logical channel used for carrying the Layer 3 message. Since time is required to receive, process, and react to each received burst, the bursts required for transmission of a Layer 3 message are usually sent in a staggered format, as schematically illustrated in FIG. 2 and as described above in connection with the IS-54B standard.

FIG. 2 shows a general example of a forward (or downlink) DCCH configured as a succession of time slots 1, 2, . . . , N, . . . included in the consecutive time slots 1, 2, . . . sent on a carrier frequency. These DCCH slots may be defined on a radio channel such as that specified by IS-54B, and may consist, as seen in FIG. 2 for example, of every n-th slot in a series of consecutive slots. Each DCCH slot has a duration that may or may not be 6.67 msec, which is the length of a DTC slot according to the IS-54B standard.

As shown in FIG. 2, the DCCH slots may be organized into superframes (SF), and each superframe includes a number of logical channels that carry different kinds of information. One or more DCCH slots may be allocated to each logical channel in the superframe. The exemplary downlink superframe in FIG. 2 includes three logical channels: a broadcast control channel (BCCH) including six successive slots for overhead messages; a paging channel (PCH) including one slot for paging messages; and an access response channel (ARCH) including one slot for channel assignment and other messages. The remaining time slots in the exemplary superframe of FIG. 2 may be dedicated to other

THIS PAGE BLANK (USPTO)

-9-

logical channels, such as additional paging channels PCH or other channels. Since the number of mobile stations is usually much greater than the number of slots in the superframe, each paging slot is used for paging several mobile stations that share some unique characteristic, e.g., the last digit of the MIN.

5 For purposes of efficient sleep mode operation and fast cell selection, the BCCH may be divided into a number of sub-channels. U.S. Patent Application No. 07/956,640 discloses a BCCH structure that allows the mobile station to read a minimum amount of information when it is switched on (when it locks onto a DCCH) before being able to access the system (place or receive a call). After
10 being switched on, an idle mobile station needs to regularly monitor only its assigned PCH slots (usually one in each superframe); the mobile can sleep during other slots. The ratio of the mobile's time spent reading paging messages and its time spent asleep is controllable and represents a tradeoff between call-set-up delay and power consumption.

15 Since each TDMA time slot has a certain fixed information carrying capacity, each burst typically carries only a portion of a Layer 3 message as noted above. In the uplink direction, multiple mobile stations attempt to communicate with the system on a contention basis, while multiple mobile stations listen for Layer 3 messages sent from the system in the downlink
20 direction. In known systems, any given Layer 3 message must be carried using as many TDMA channel bursts as required to send the entire Layer 3 message.

Digital control and traffic channels are desirable for these and other reasons described in U.S. Patent Application No. 08/147,254, entitled "A Method for Communicating in a Wireless Communication System", which was
25 filed on November 1, 1993, and which is incorporated in this application by reference. For example, they support longer sleep periods for the mobile units, which results in longer battery life. Although IS-54B provides for digital traffic channels, more flexibility is desirable in using digital control channels having expanded functionality to optimize system capacity and to support hierarchical
30 cell structures, i.e., structures of macrocells, microcells, picocells, etc. The

THIS PAGE BLANK (USPTO)

-10-

term "macrocell" generally refers to a cell having a size comparable to the sizes of cells in a conventional cellular telephone system (e.g., a radius of at least about 1 kilometer), and the terms "microcell" and "picocell" generally refer to progressively smaller cells. For example, a microcell might cover a public indoor or outdoor area, e.g., a convention center or a busy street, and a picocell might cover an office corridor or a floor of a high-rise building. From a radio coverage perspective, macrocells, microcells, and picocells may be distinct from one another or may overlap one another to handle different traffic patterns or radio environments.

FIG. 3 is an exemplary hierarchical, or multi-layered, cellular system. An umbrella macrocell 10 represented by a hexagonal shape makes up an overlying cellular structure. Each umbrella cell may contain an underlying microcell structure. The umbrella cell 10 includes microcell 20 represented by the area enclosed within the dotted line and microcell 30 represented by the area enclosed within the dashed line corresponding to areas along city streets, and picocells 40, 50, and 60, which cover individual floors of a building. The intersection of the two city streets covered by the microcells 20 and 30 may be an area of dense traffic concentration, and thus might represent a hot spot.

FIG. 4 represents a block diagram of an exemplary cellular mobile radiotelephone system, including an exemplary base station 110 and mobile station 120. The base station includes a control and processing unit 130 which is connected to the MSC 140 which in turn is connected to the PSTN (not shown). General aspects of such cellular radiotelephone systems are known in the art, as described by the above-cited U.S. patent applications and by U.S. Patent No. 5,175,867 to Wejke et al., entitled "Neighbor-Assisted Handoff in a Cellular Communication System," and U.S. Patent Application No. 07/967,027 entitled "Multi-mode Signal Processing," which was filed on October 27, 1992, both of which are incorporated in this application by reference.

The base station 110 handles a plurality of voice channels through a voice channel transceiver 150, which is controlled by the control and processing

THIS PAGE BLANK (USPTO)

-11-

unit 130. Also, each base station includes a control channel transceiver 160, which may be capable of handling more than one control channel. The control channel transceiver 160 is controlled by the control and processing unit 130. The control channel transceiver 160 broadcasts control information over the control channel of the base station or cell to mobiles locked to that control channel. It will be understood that the transceivers 150 and 160 can be implemented as a single device, like the voice and control transceiver 170, for use with DCCHs and DTCs that share the same radio carrier frequency.

The mobile station 120 receives the information broadcast on a control channel at its voice and control channel transceiver 170. Then, the processing unit 180 evaluates the received control channel information, which includes the characteristics of cells that are candidates for the mobile station to lock on to, and determines on which cell the mobile should lock. Advantageously, the received control channel information not only includes absolute information concerning the cell with which it is associated, but also contains relative information concerning other cells proximate to the cell with which the control channel is associated, as described in U.S. Patent No. 5,353,332 to Raith et al., entitled "Method and Apparatus for Communication Control in a Radiotelephone System," which is incorporated in this application by reference.

As noted above, one of the goals of a digital cellular system is to increase the user's "talk time", i.e., the battery life of the mobile station. To this end, U.S. Patent Application No. 07/956,640 discloses a digital forward control channel (base station to mobile station) that can carry the types of messages specified for current analog forward control channels (FOCCs), but in a format which allows an idle mobile station to read overhead messages when locking onto the FOCC and thereafter only when the information has changed; the mobile sleeps at all other times. In such a system, some types of messages are broadcast by the base stations more frequently than other types, and mobile stations need not read every message broadcast.

-12-

Also, Application No. 07/956,640 shows how a DCCH may be defined alongside the DTCs specified in IS-54B. For example, a half-rate DCCH could occupy one slot and a full-rate DCCH could occupy two slots out of the six slots in each TDMA frame. For additional DCCH capacity, additional half-rate or full-rate DCCHs could replace DTCs. In general, the transmission rate of a DCCH need not coincide with the half-rate and full-rate specified in IS-54B, and the length of the DCCH time slots need not be uniform and need not coincide with the length of the DTC time slots.

Although the above-described communication systems are highly beneficial and are markedly different from previous systems, Applicants' communication system is capable of broadcasting special messages to the mobile stations without affecting other aspects of its performance.

SUMMARY

According to an exemplary embodiment of the present invention, broadcast SMS systems can be provided wherein a plurality of messages are transmitted over one or more sub-channels of a logical S-BCCH channel that have a fixed, time multiplexed format relative to other logical channels. Message attributes are specified on a per message basis so that a mobile station will look at the attributes of each message to determine whether or not that message should be read by that mobile station. In this exemplary embodiment, new sub-channels are added by the system as needed to support the number of messages to be transmitted at any given time.

According to another exemplary embodiment of the present invention, broadcast SMS systems can be provided wherein the sub-channel ordering is more flexible since it is not provided in a fixed, time multiplexed format. Message attributes are associated on a sub-channel basis rather than a per message basis. In this way, messages can be grouped into categories based upon subsets of different message attributes and transmitted based upon their grouping.

THIS PAGE BLANK (USPTO)

-13-

Similarly, mobile messages associated with those groups whose attribute(s) match those associated with a subscriber.

BRIEF DESCRIPTION OF THE DRAWINGS

The features and advantages of Applicants' invention will be understood
5 by reading this description in conjunction with the drawings, in which:

FIG. 1 illustrates a plurality of Layer 3 messages, Layer 2 frames, and Layer 1 channel bursts in a communication system;

FIG. 2 is a generalized view of a digital control channel (DCCH) having time slots which are grouped into superframes;

10 FIG. 3 illustrates a typical multi-layered cellular system employing umbrella macrocells, microcells and picocells;

FIG. 4 represents an exemplary implementation of an apparatus for a radiotelephone system according to the present invention;

FIG. 5 shows a hyperframe structure;

15 FIG. 6 shows the logical channels of the DCCH;

FIG. 7 shows an exemplary TDMA frame structure;

FIGS. 8a-8c show exemplary slot formats on the DCCH;

FIG. 9 shows the partitioning of data before channel encoding;

FIG. 10 shows a paging frame structure;

20 FIG. 11 shows an SMS frame structure;

FIG. 12 shows an example of SMS sub-channel multiplexing; and

FIGS. 13a-13c show S-BCCH Layer 2 frames according to a first exemplary broadcast SMS embodiment; and

25 FIGS. 14a-14d show S-BCCH Layer 2 frames according to a second exemplary embodiment.

DETAILED DESCRIPTION

The following description is in terms of a cellular radiotelephone system, but it will be understood that Applicants' invention is not limited to that

THIS PAGE BLANK (USPTO)

-14-

environment. Also, the following description is in the context of TDMA cellular communication systems, but it will be understood by those skilled in the art that the present invention may apply to other digital communication applications such as Code Division Multiple Access (CDMA). The physical channel may be, for
5 example, a relatively narrow band of radio frequencies (FDMA), a time slot on a radio frequency (TDMA), a code sequence (CDMA), or a combination of the foregoing, which can carry speech and/or data, and is not limited to any particular mode of operation, access technique, or system architecture.

In one aspect of Applicants' invention, communication between mobile
10 stations and base stations is structured into successions of different kinds of logical frames. FIG. 5 illustrates the frame structure of a forward (base station to mobile station) DCCH and shows two successive hyperframes (HF), each of which preferably comprises a respective primary superframe (SF) and a respective secondary superframe. It will be recognized, of course, that a
15 hyperframe could include more than two superframes.

Three successive superframes are illustrated in FIG. 5, each comprising a plurality of time slots that are organized as logical channels F-BCCH, E-BCCH, S-BCCH, and SPACH that are described in more detail below. At this point, it is sufficient to note that each superframe in a forward DCCH includes a
20 complete set of F-BCCH information (i.e., a set of Layer 3 messages), using as many slots as are necessary, and that each superframe begins with a F-BCCH slot. After the F-BCCH slot or slots, the remaining slots in each superframe include one or more (or no) slots for the E-BCCH, S-BCCH, and SPACH logical channels.

Referring to FIG. 5, and more particularly to FIG. 6, each superframe of
25 the downlink (forward) DCCH preferably comprises a broadcast control channel BCCH, and a short-message-service/paging/access channel SPACH. The BCCH comprises a fast BCCH (the F-BCCH shown in FIG. 5); an extended BCCH (the E-BCCH); and a short-message-service BCCH (the S-BCCH), all of which are
30 used, in general, to carry generic, system-related information from the base

THIS PAGE BLANK (USPTO)

-15-

stations to the mobiles. The BCCH is unidirectional, shared, point-to-multipoint, and unacknowledged. The SPACH comprises a short-message-service channel SMSCH, a plurality of paging channels PCH, and an access response channel ARCH, which are used to send information to specific mobile stations relating to

5 short-message-service point-to-point messages (SMSCH), paging messages (PCH), and messages responding to attempted accesses (ARCH) as described below. The SPACH is unidirectional, shared, and unacknowledged. The PCH may be considered point-to-multipoint, in that it can be used to send paging messages to more than one mobile station, but in some circumstances the PCH is

10 point-to-point. The ARCH and SMSCH are generally point-to-point, although messages sent on the ARCH can also be addressed to more than one mobile station.

For communication from the mobile stations to the base stations, the reverse (uplink) DCCH comprises a random access channel RACH, which is

15 used by the mobiles to request access to the system. The RACH logical channel is unidirectional, shared, point-to-point, and acknowledged. All time slots on the uplink are used for mobile access requests, either on a contention basis or on a reserved basis. Reserved-basis access is described in U.S. Patent Application No. 08/140,467, entitled "Method of Effecting Random Access in a Mobile

20 Radio System", which was filed on October 25, 1993, and which is incorporated in this application by reference. One important feature of RACH operation is that reception of some downlink information is required, whereby mobile stations receive real-time feedback for every burst they send on the uplink. This is known as Layer 2 ARQ, or automatic repeat request, on the RACH. The

25 downlink information preferably comprises twenty-two bits that may be thought of as another downlink sub-channel dedicated to carrying, in the downlink, Layer 2 information specific to the uplink. This flow of information, which can be called shared channel feedback, enhances the throughput capacity of the RACH so that a mobile station can quickly determine whether any burst of any

THIS PAGE BLANK (USPTO)

-16-

access attempt has been successfully received. Other aspects of the RACH are described below.

5 The F-BCCH logical channel carries time-critical system information, such as the structure of the DCCH, other parameters that are essential for accessing the system, and an E-BCCH change flag that is described in more detail below; as noted above, a complete set of F-BCCH information is sent in every superframe. The E-BCCH logical channel carries system information that is less time-critical than the information sent on the F-BCCH; a complete set of E-BCCH information (i.e., a set of Layer 3 messages) may span several
10 superframes and need not be aligned to start in the first E-BCCH slot of a superframe. The S-BCCH logical channel carries short broadcast messages, such as advertisements and information of interest to various classes of mobile subscriber, and possibly system operation information, such as change flags for the other logical channels. An important aspect of Applicants' invention is that
15 the S-BCCH decouples the system overhead information sent on the F-BCCH and E-BCCH from the broadcast message service (S-BCCH), obtaining maximum system flexibility. It would be possible to omit the S-BCCH and send its messages on the E-BCCH or even the F-BCCH, but doing so would delay the delivery of important system information since the SMS messages would be
20 intermingled with the system overhead messages.

As for the SPACH slots, they are assigned dynamically to the SMSCH, PCH, and ARCH channels based on transmitted header information. The SMSCH logical channel is used to deliver short messages to a specific mobile station receiving SMS services. The PCH logical channel carries paging
25 messages and other orders to the mobiles, such as the F-BCCH change flag described above and in U.S. Patent Application No. 07/956,640. Mobile stations are assigned respective PCH slots in a manner described in more detail below. A mobile station listens to system responses sent on the ARCH logical channel upon successful completion of the mobile's access on a RACH. The ARCH may

THIS PAGE BLANK (USPTO)

-17-

be used to convey AVC or DTC assignments or other responses to the mobile's attempted access.

An important aspect of exemplary embodiments is that every PCH slot in the primary superframe of a hyperframe is repeated in the secondary superframe of that hyperframe. This is called "specification guaranteed repeat". Thus, once
5 a mobile station has read the BCCH information, it can enter sleep mode after determining, based on its MIN or some other distinguishing characteristic, which single PCH slot it is to monitor for a paging message. Then, if the mobile station properly receives a paging message sent in its PCH slot in a primary
10 superframe, the mobile can sleep through the entire associated secondary superframe, thereby increasing the life of its batteries. If and only if the mobile station cannot correctly decode its assigned PCH slot in a primary superframe, the mobile reads the corresponding PCH slot in the associated secondary superframe.

15 It should be understood, however, that the mobile station may read its PCH slot in only one of the superframes, either primary or secondary, for a variety of reasons, whether or not the slot is correctly decoded. This may be permitted to maximize the mobile's sleep time. Also, after the mobile has read its PCH slot in one of the superframes (for example, a primary superframe), the
20 mobile may monitor other control channels during at least part of the time until the next (primary) superframe without missing a page on the first control channel. Indeed, the mobile may even read a paging slot on another control channel. This enables cell reselection to be carried out smoothly and avoids the mobile's being blind to pages during such reselection. It will be recognized that
25 reselection is facilitated when the two control channels are synchronized, at least to the extent that a time offset between their superframes is known, which is information that may be provided on the E-BCCH for example.

One aspect of a DCCH as described in U.S. Patent Application No. 07/956,640 is that the F-BCCH slots in successive superframes carry the
30 same information until change flags transmitted in the PCH slots toggle, or

THIS PAGE BLANK (USPTO)

-18-

otherwise change value in a predetermined way. This feature is also provided in the systems and methods described in this application. Also, the E-BCCH and S-BCCH information may span both superframes in a hyperframe, and even several hyperframes, which represents a tradeoff between BCCH bandwidth (i.e., the number of slots needed for sending a complete set of BCCH messages) and the time required for a full cycle of messages sent. The toggling of a change flag in the PCH slot indicates that new data will be found on the F-BCCH sent in the following superframe. In this way, once a mobile station has read the BCCH information on a DCCH, the mobile need awaken only to read its assigned PCH slot; when the change flag in its PCH slot toggles, the mobile learns that it must either awaken or stay awake to re-acquire the F-BCCH, which has changed; if the mobile determines that the change flag has not toggled, it is not necessary for the mobile to read the F-BCCH. This also increases the mobile's sleep time, and battery life.

In a similar way, the F-BCCH slots may include E-BCCH change flags indicating that the system has changed the E-BCCH information. In response to an E-BCCH change flag, the mobile would stay awake to read the E-BCCH slots. It will be understood that the change of the E-BCCH change flag in the F-BCCH slots is "new data" to be found on the F-BCCH that would be indicated by the F-BCCH change flag transmitted in the PCH slots. The mobile station preferably stores the value of the E-BCCH change flag transmitted in the F-BCCH slots before reading the E-BCCH. After the mobile station has acquired the relevant information (which may be dependent on the specific task the mobile is engaged in), the mobile reads the E-BCCH change notification flag again. The process of updating/initiating the E-BCCH message set can be considered successful when the E-BCCH change flag is the same before and after the mobile reads the E-BCCH.

Among the other important features of Applicants' invention, is that information is not interleaved among successive slots, although as described below, information may be interleaved among fields in the same slot. Also as

THIS PAGE BLANK (USPTO)

-19-

described below, the downlink information is advantageously encoded by error correction codes for immunity to channel impairments, for example a convolutional rate-1/2 code. It is desirable not to use "too much" encoding like a convolutional rate-1/4 code, however, because the number of user data bits sent in any given channel burst would be low. Also, such encoding is not needed because the BCCH information is repeated in every superframe and certain transactions can use ARQ. The BCCH and PCH cannot use ARQ, of course, but using a single type of coding is advantageous because it reduces equipment complexity. Therefore, to obtain sufficient protection, somewhat less encoding is combined with the time diversity provided by specification guaranteed repeat for the PCH. This combination is also beneficial for sleep mode performance.

The combination of these features results in a communication system that has good immunity to errors at the same time that it permits, on average, long mobile sleep times. It will be appreciated that the guaranteed repeats of the PCH slots provide time diversity, yielding an improved immunity to errors due to Rayleigh fading that is provided in previous systems by rate-1/4 encoding and inter-burst interleaving. (Of course, specification guaranteed repeat is not an option for speech slots.) Applicants' combination of these features, however, results in a communication system that permits a mobile that has successfully decoded its PCH slot in a primary superframe to sleep through all of the PCH slots in the corresponding secondary superframe. It will be recognized that the a mobile's assigned PCH slots are temporally separated by many times the duration of such a slot (6.67 msec).

The BCCH information sent in one or more slots of the DCCH comprises information about the serving system and the desired behavior of the mobile station when operating in this system. The overhead information would include, for example, indications of the following: (1) the paging slot to which the mobile station is assigned; (2) whether the mobile station is allowed to make and receive any calls through this base station or is restricted to only emergency calls; (3) the power level to be used for transmitting to this base station; (4) the

THIS PAGE BLANK

-20-

identity of the system (home system or visited system); (5) whether or not to use an equalizer for compensating distortion and attenuation effects of the radio channel on the transmitted signal; and (6) the location of other DCCHs (frequencies, time slots, time offsets of other DCCHs' superframes with respect to superframes of current DCCH) of neighboring base stations. A DCCH of a neighboring base station may be selected because the DCCH signal received from this base station is too weak or for some other reason, e.g., the signal from another base station is stronger than the signal from this base station.

When a mobile station locks onto the DCCH, the mobile station first reads the overhead information to determine the system identity, call restrictions, etc.; the locations of the DCCHs of the neighboring base stations (the frequencies, time slots, etc., on which these DCCHs may be found); and its paging slot in the superframe (the DCCH slot assigned to the paging frame class to which the mobile station belongs). The relevant DCCH frequencies are stored in memory, and the mobile station then enters sleep mode. Thereafter, the mobile station "awakens" once every hyperframe, depending on the mobile's paging frame class, to read the assigned paging slot, and then returns to sleep.

The F-BCCH information transmitted in every superframe allows a mobile station to read other information in the superframe, to access the system, or to quickly find the best serving cell, when first locking onto a DCCH. For example, certain basic information about the low-layer structure of the DCCH must be read by a mobile station before any other information in the superframe can be read. This basic information includes, for example, a superframe period (number of DCCH slots), whether the DCCH is half-rate or full-rate, the DCCH format (which slot(s) in a TDMA frame), the location of other BCCH channels, the location of the assigned PCH, and whether the mobile station receiver should use an equalizer. Other types of information should also be sent rather often so that a mobile station can quickly accept or reject a particular DCCH. For example, information about the availability and data capability of a cell (the cell may be available only to a closed user group or may not be capable of handling

THIS PAGE BLANK (USPTO)

-21-

data transmissions from a mobile station), the identity of the system and the cell, etc., may be sent in every superframe. For accelerating system accesses, it would be sufficient for a mobile station to read only system access rules sent on the F-BCCH.

- 5 The E-BCCH is assigned a system-controlled, fixed number of slots in each superframe, but a long cycle, or set of messages, sent on the E-BCCH may span several superframes; hence, the number E-BCCH slots in each superframe can be much less than the number of slots needed to carry the long cycle, or set of messages. If there are not enough E-BCCH slots in a superframe to
- 10 accommodate all E-BCCH messages, subsequent superframes are used. Mobile stations are notified through the F-BCCH as described above of the number and location of E-BCCH slots assigned in each superframe. A start-of-E-BCCH marker may be sent in the current F-BCCH (or S-BCCH) to inform the mobile stations that the current superframe contains the start of an E-BCCH message.
- 15 With the E-BCCH, long and/or sporadic information may be sent on the DCCH without affecting the organization of the superframe, e.g., PCH assignments, or the DCCH capacity. For example, the list of DCCHs of neighboring base stations may be sent on the E-BCCH. Such a list can be rather large, including the locations of, say, ten other DCCHs. Such a list would
- 20 require several slots to transmit, and these slots may be spread out over the E-BCCH of several superframes instead of taking up a large portion of one superframe. In this way, BCCH overhead is traded off for a larger number of paging slots (and consequent increased paging capacity).

Layer 1 FORMAT

- 25 An exemplary organization of the information transmitted on each radio channel, i.e., the channel bursts, or time slots, in accordance with Applicants' invention is shown in FIG. 7. This organization is similar to that specified by the IS-54B standard. The consecutive time slots on a radio channel are organized in TDMA frames of six slots each and TDMA blocks of three slots each so that

THIS PAGE BLANK (USPTO)

-22-

a plurality of distinct channels can be supported by a single radio carrier frequency. Each TDMA frame has a duration of 40 msec and supports six half-rate logical channels, three full-rate logical channels, or various combinations between these extremes by interchanging one full-rate channel and two half-rate channels as indicated in the following table. Each slot has a duration of 6.67 msec and carries 324 bits (162 symbols), which have positions in each slot that are conventionally consecutively numbered 1-324.

Number of Slots	Used Slots	Rate
1	1	half
2	1,4	full
4	1,4,2,5	2 full
6	1,4,2,5,3,6	3 full

As explained above, each superframe comprises a predetermined number of successive time slots (full-rate) of a DCCH. Since a complete set of F-BCCH information is sent in each superframe and since the first slot of each superframe is a F-BCCH slot, each superframe is the interval between such initial F-BCCH slots. It is currently preferred that each superframe consist of thirty-two such time slots, which are distributed among the logical channels F-BCCH, E-BCCH, S-BCCH, and SPACH as illustrated in FIG. 5 for example. Thus, the duration of each logical superframe is simply 32 TDMA blocks/superframe * 20 msec/TDMA block = 640 msec, which spans 96 consecutive physical time slots on the radio channel.

It will be appreciated that this selection represents a balance of several factors that Applicants' currently deem most useful. For example, using thirty-two slots, which is an integer power of two, simplifies the implementation of various counters in existing hardware that is based on binary signal processing. Also, using thirty-two-slot superframes balances call set-up delay against paging

THIS PAGE BLANK (USPTO)

-23-

channel (and other channel) capacity. For a given amount of BCCH information to be transmitted, using longer superframes would increase paging capacity, but would also increase the average set-up delay; using shorter superframes would decrease the average set-up delay to an extent, but would also decrease paging capacity and devote a greater proportion of each superframe to overhead information. Different balances can be struck that would nevertheless fall within the spirit of Applicants' invention.

In order to locate each time slot in each superframe and thus provide the enhanced sleep capabilities made available by Applicants' invention, a superframe phase (SFP) count, which increments by one for each full-rate DCCH slot in a given superframe, is included as part of the information broadcast in each downlink DCCH slot. The SFP value sent in the first slot (an F-BCCH slot) of each superframe may be assigned the value 0; the next slot of the same logical DCCH is assigned an SFP value of 1, etc. Thus, for a system using superframes of thirty-two slots each, the SFP value increments modulo-32, and the SFP value sent in each slot requires five bits. For a half-rate DCCH, only half of the values (e.g., 0, 2, 4, . . . , 30) need be used to identify the slots in each superframe of the DCCH.

It will be appreciated that such a modulo-32 up-counter could be replaced by a modulo-32 down-counter, and for a communication system that does not employ superframes having a fixed number of time slots, the modulo-32 up-counter would be replaced by a down counter for indicating the next occurrence of the F-BCCH, or other desired overhead information. It is only necessary for the information in a slot to include some indication of that slot's position in time with respect to the next occurring time slot carrying the important overhead information. It is also desirable that the information indicate the start of the superframe/hyperframe/paging-frame structures, i.e., that the boundaries of the frame structures all be synchronized with the next occurring time slot carrying the important overhead information, but such synchronization is not necessary.

THIS PAGE BLANK (USPTO)

-24-

Two possible formats for the information sent in the slots of the reverse DCCH are shown in FIGS. 8a and 8b, and a preferred information format in the slots of the forward DCCH is shown in FIG. 8c. These formats are substantially the same as the formats used for the DTCs under the IS-54B standard, but new functionalities are accorded to the fields in each slot in accordance with Applicants' invention. In FIGS. 8a-8c, the number of bits in each field is indicated above that field.

In general, messages (Layer 2 user data bits) to be carried by the slots are mapped onto the two DATA fields sent in each slot, and in the downlink slots, encoded SFP values are sent in the CSFP fields that uniquely identify each slot according to each slot's relative position in its superframe. Also in the downlink slots, the BRI, R/N, and CPE fields contain the information used in the random access scheme for Layer 2 ARQ on the RACH; comparable Layer 2 ARQ fields could be included in the uplink slots. In the forward DCCH (FIG. 8c), the DATA fields total 260 bits in length, the CSFP field carries twelve bits, and the BRI, R/N, CPE fields for shared channel feedback total twenty-two bits. In the reverse DCCH, the DATA fields total either a normal 244 bits in length (FIG. 8a) or an abbreviated 200 bits (FIG. 8b).

The bits sent in the G, R, PREAM, SYNC, SYNC+, and AG fields are used in a conventional way to help ensure accurate reception of the CSFP and DATA fields, e.g., for synchronization, guard times, etc. For example, the SYNC field would be the same as that of a DTC according to IS-54B and would carry a predetermined bit pattern used by the base stations to find the start of the slot. Also, the SYNC+ field would include a fixed bit pattern to provide additional synchronization information for the base stations, which would set their receiver gains during the PREAM field so as to avoid signal distortion.

Referring again to FIG. 8c, the CSFP field in each DCCH slot conveys the SFP value that enables the mobile stations to find the start of each superframe. The SFP values are preferably encoded with a (12,8) code, similar to the way the DVCC is encoded according to the IS-54B standard; thus, the

THIS PAGE BLANK (USPTO)

-25-

CSFP field is preferably twelve bits in length, and the unencoded SFP consists of eight bits. Encoding the SFP values in this way has the advantage of using the hardware and software already present in the mobile phone for handling the DVCC. Also, the four check bits are preferably inverted, enabling a mobile to

5 use the information sent in the CSFP field to discriminate between a DCCH and a DTC since the CSFP of a DCCH and the CDVCC of a DTC have no common codewords. Other ways to discriminate DCCHs from DTCs are described in U.S. Patent Application No. 08/147,254. In view of the importance of the SFP to the operation of the system, a mobile station might decode the CSFPs in

10 several slots in order to ensure accuracy since the CSFP in any individual slot is less well protected by encoding and time diversity than the Layer 3 message in the DATA fields.

When each superframe includes thirty-two slots, the three most significant bits in each eight unencoded SFP bits may be set to zero. It will be appreciated

15 that the unused SFP bits could be used for particular purposes, e.g., to handle superframes consisting of more than thirty-two slots each or for Layer 1 power control messages. Also, the three unused SFP bits could be used, either alone or in combination with other unused (reserved) bits transmitted in each slot, for increasing the redundancy or strengthening the error correction coding of

20 the SFP, if determined to be necessary. It will be appreciated that the SFP information could be included in the Layer 2 frame header information, rather than in separate Layer 1 fields as shown.

Also, in a system using thirty-two-slot superframes, it is currently preferred that the sixteen CRC, or check, bits in the Layer 2 frames sent in the

25 BCCH slots are inverted, while the sixteen check bits in the Layer 2 frames sent in the SPACH slots are not inverted. Using the check bits in this way is advantageous in some situations where it is necessary to re-assign a mobile station to another paging slot. For example, if a system has been using twelve slots of a thirty-two-slot superframe for the BCCH and wants to use thirteen slots

30 for the BCCH, mobile stations assigned to the first paging slot after the BCCH

THIS PAGE BLANK (USPTO)

-26-

slots must be informed that they should monitor another paging slot. The mobiles could obtain this information by decoding one or two bits that would identify the type of slot being decoded, but at a cost of reduced bandwidth. In Applicants' system, the mobile stations will recognize that something has
5 changed when they spot the inverted CRC bits, and in response they will re-read the F-BCCH, including the new DCCH structure message.

A hyperframe count and a primary SF indicator are also preferably included in the information carried by the BCCH slots; in particular as described in more detail below, these information elements are included in the DCCH
10 structure message carried by the F-BCCH. The hyperframe count identifies which hyperframe of a higher-level structure of paging frames and SMS frames is currently being broadcast, as described below in connection with FIG. 10. In accordance with Applicants' invention, four paging frame classes and/or a plurality of broadcast SMS sub-channels may be provided as described below.
15 The primary superframe indicator is a single bit that toggles to indicate whether the current superframe is the primary or the secondary superframe in the current hyperframe; when its value is zero, the current superframe may be the primary, and vice versa. In one embodiment of Applicants' invention, the hyperframe count counts modulo-12.

20 FIG. 9 shows a currently preferred partitioning of the Layer 2 user data bits before channel encoding. The DATA fields in the logical channels BCCH, SPACH, and RACH (normal and abbreviated) preferably use 1/2-rate convolutional encoding; thus, the two DATA fields in each forward DCCH slot carry 109 plaintext, or unencoded, BCCH or SPACH bits; and the two DATA
25 fields in each reverse DCCH slot carry either a normal 101 plaintext RACH bits or an abbreviated 79 plaintext RACH bits. Also, the encoded user data bits are preferably interleaved between the two DATA fields in each slot, but they are not interleaved among DATA fields in different slots in order to enable the longer sleep times available from Applicants' invention. Interleaving may be

THIS PAGE BLANK (USPTO)

-27-

done according to suitable convenient matrices, like those used under the IS-54B standard.

Different DCCHs may be assigned to different radio channel frequencies, and a different number of slots may be allocated to the BCCH on each DCCH.

5 Layer 2/3 information may also be different for each DCCH, but this is not required. In an embodiment in which each DCCH includes its own BCCH, much information is redundant from DCCH to DCCH, resulting in a loss of paging capacity. In another embodiment, DCCHs may be organized in master-slave relationships, in which full BCCH information would be available only on
10 the master DCCH; a mobile monitoring a slave DCCH would acquire its BCCH information by changing to its slave's corresponding master DCCH. It is currently preferred that each frequency carry a full set of BCCH information and a mobile station always acquire all its BCCH information on the same frequency as its assigned PCH channel.

15 The structure of the DCCH transmitted on the F-BCCH in the first slot of each superframe is the most important information for a mobile to acquire. An advantageous DCCH structure message comprises the information elements listed in the following table.

20	Information Element	I E Type	Bit Length
	Message type	M	8
	Number of F-BCCH slots	M	2
	Number of E-BCCH slots	M	3
	Number of S-BCCH slots	M	4
	Number of Skipped slots	M	3
25	E-BCCH change notification flag	M	1
	Hyperframe count	M	4
	Primary superframe indicator	M	1
	Number of DCCH slots on this frequency	M	2
	MAX_SUPPORTED_PFC	M	2
30	PCH_DISPLACEMENT	M	3

THIS PAGE BLANK (USPTO)

-28-

Additional DCCH frequencies	O	23-114
		Total = 33-147

M = Mandatory

O = Optional

As described above, the mobile station normally monitors only one of the PCH slots in a superframe to minimize power consumption, or battery drain. Since some paging messages may be longer than the capacity of a single time slot, each PCH slot carries a PCON bit that may be set to cause the assigned mobile station to read additional SPACH slots, the number of which is advantageously indicated by a parameter PCH_DISPLACEMENT sent on the F-BCCCH. The additional slots to be read preferably are separated by at least 40 msec (one TDMA frame) from the assigned PCH slot for both full- and half-rate DCCHs. For example, for a full-rate DCCH, the mobile station would attempt to read every other SPACH slot up to the number indicated by the PCH_DISPLACEMENT parameter. This is advantageous in that it reduces the trunking loss caused by the creation of the several distinct paging channels. Also, using every other SPACH slot in this way gives a mobile station time for processing its received information to determine whether it must read additional slots. If every SPACH slot were used instead of at least every other one, a mobile station having a slow processing unit might not complete processing by the time the next SPACH slot occurred; since the mobile would not yet be aware that the PCON bit was set, it would have to read the next slot even if that were unnecessary and sleep mode performance would suffer.

Also, the transmission of long ARCH or SMSCH messages to a first mobile station may be interrupted to allow for the transmission of messages to a second mobile station. Each interruption of an ARCH or SMSCH message by another SPACH message may be limited to no more than a predetermined number *n* of time slots, or by Layer 3 timeout for SMSCH or ARCH messages. It will be understood that Layer 3 timeout refers to the common practice of

THIS PAGE BLANK (USPTO)

-29-

waiting for a response to a Layer 3 message only for a predetermined period. The number of interruptions each mobile station may suffer may also be limited.

Ordinarily, the probability of a successful transmission of a Layer 3 message is inversely related to the length of the message. Since the probability
5 can be quite small for long messages, a simple-minded system would spend much of its time re-transmitting or re-reading entire messages that were not properly received. In Applicants' system, Layer 3 paging and broadcast SMS messages are mapped onto Layer 2 frames, and these are organized in structures called
10 paging frames and SMS frames, respectively. For the BCCH, if a Layer 2 frame is not received properly, it is not necessary to re-read the entire Layer 3 message but only the improperly received Layer 2 frame. The ARCH and RACH can use ARQ.

In accordance with an aspect of Applicants' invention, the superframes and hyperframes on each DCCH are grouped into a succession of paging frames,
15 each of which includes an integer number of hyperframes and is a member of one of a plurality of paging frame classes; hence, the PCH slots have the paging frame structure. In accordance with one aspect of Applicants' invention, the mobile station reads its assigned PCH slot only in the hyperframes of its allocated paging frame class. (As described above, each mobile station is
20 allocated a specific PCH sub-channel within a paging frame based preferably on the mobile's IS-54B MIN identity.) In many cases, mobile stations would be allocated a paging frame class that would cause the mobiles to read their assigned PCH slots in each hyperframe; this minimizes call set-up time and sleep
25 duration. But other paging classes would have the mobiles read PCH slots in more widely separated hyperframes, delaying call set-ups but increasing sleep times to as much as 123 seconds for some types of paging frame structure. Thus, it will be appreciated that PCH slots are included in every superframe but the PCH slot assigned to a given mobile may not be.

Referring to the exemplary table shown in FIG. 10, primary and
30 secondary PCH slots p and s in the primary and secondary superframes,

THIS PAGE BLANK (USE TO)

-30-

respectively, of each hyperframe may be grouped in one of four PF classes PF_1 - PF_4 , which are distinguished by how frequently the PCH slot information is repeated. Class PF_1 may be called the "lowest" PF class because PCHs in this class repeat their information with the lowest duration between repeats; in
5 FIG. 10, the PCH slot is repeated in each successive hyperframe (i.e., in every successive superframe). Class PF_4 may be called the "highest" PF class because PCHs in this class repeat their information with the highest duration between repeats; in FIG. 10, the PCH slot is repeated only every fourth hyperframe. As described above, the PCH information in a primary superframe is guaranteed to
0 be repeated in the corresponding secondary superframe. In FIG. 10 for paging frame class $PF(i)$, where $i = 2, 3, 4$, only the PCH assignments which are aligned to HF_0 are shown for illustration purposes.

In the embodiment illustrated by FIG. 10, there are only four paging frame classes that are linearly related, yielding maximum sleep times of eight
15 superframes, or 5.12 seconds. Longer sleep times can be obtained by providing more classes that are exponentially related. For example, sleep times of 123 seconds are obtained in a system having eight paging frame classes in which the delays double from class to class. It will be understood that long sleep times can result in access delays that are unacceptable for typical telephone use; for
20 example, most callers attempting to reach a mobile would be unwilling to wait 123 seconds after dialing the mobile's number for contact to be established. Nevertheless, such delays may be tolerable in some cases, such as remote polling of equipment like soft-drink dispensers.

In an embodiment using the table illustrated in FIG. 10, the least common
25 multiple of the indices of the four paging frame classes is twelve; this is the reason that the HF counter counts modulo-12, as described above.

Three other terms used in describing the operation of the PF classes are default PF class, assigned PF class, and current PF class. The default PF class is the class assigned to the mobile station when its subscription to the system is
30 entered. If the default PF class happens to be higher than the highest class

THIS PAGE BLANK (USPTO)

-31-

supported by a DCCH, as defined by the parameter MAX_SUPPORTED_PFC in the DCCH structure message, the mobile would use the PF class defined by MAX_SUPPORTED_PFC. The assigned PF class refers to a PF class assigned to the mobile by the system, for example in the system's response to a registration request by the mobile. The PF class actually used during a communication may be called the current PF class.

According to other exemplary embodiments of the present invention, broadcast short message service (SMS) can be supported by way of logical sub-channeling in a variety of ways. Two examples will be discussed in detail, with other modifications and adaptations described after the detailed examples.

In one exemplary embodiment of Applicants' invention, depicted in FIGS. 11-13, the S-BCCH slots in successive superframes are grouped into a succession of fixed-length SMS frames, each preferably consisting of twenty-four superframes (twelve hyperframes) as shown in FIG. 11. This S-BCCH frame structure enables messages to be sent with highly variable periodicity without sacrificing capacity, and as described below, it avoids requiring the mobile stations to re-read constantly the entire S-BCCH information when only one of the many messages sent has changed. Also, choosing an SMS frame structure that is conveniently related to the paging frame class structure enables counters that are already in use for one purpose (paging) to be re-used for another purpose (SMS broadcast messaging).

The SMS frames are advantageously divided into a plurality of sub-channels, each having its own repetition cycle defined in terms of units of possible SMS frames. For most practical situations, the sub-channel repetition time should not be too long. In a manner similar to the handling of the F-BCCH change flag described above, a mobile station is informed of a change in the contents of particular sub-channels through an SMS transition flag (TF) included in its PCH slot information.

Currently, four SMS sub-channels are preferred for this exemplary embodiment, and the SMS sub-channels are sub-multiplexed on the S-BCCH

THIS PAGE BLANK (USPTO)

-32-

channel in units of SMS frames, e.g., SMS frame SMS(i), where $i = 1, \dots, N$, as illustrated in FIG. 12. It will be understood that each (Layer 1) time slot carries a respective SMS frame and that a Layer 3 SMS message can span several SMS frames.

- 5 An SF number is advantageously derived from the hyperframe count and primary superframe indicator sent on the BCCH as follows:

$$\text{SF number} = 2 \cdot \text{HF count} + \text{primary SF indicator}.$$

- The first S-BCCH slot(s) within each SMS frame (superframe 0) would contain a header that describes the structure of the SMS sub-channel. As noted above, the number of superframes within each SMS frame is fixed for this exemplary embodiment, and thus the number of slots assigned to the SMS frame are 0, 24, 48, 72, . . . (full-rate), depending on how many slots per superframe are assigned to S-BCCH. The SMS frame is aligned to start at HF counter equal to zero and in a primary superframe to help the mobile synchronize to the SMS frame structure. In this way, SMS frames are synchronized to the hyperframes and superframes, although it will be appreciated that the start of an SMS frame is offset from the start of a hyperframe (or a primary superframe) since the S-BCCH slots are not the first slots in a superframe. Furthermore, regardless of how many paging frame classes are supported, the system increments the hyperframe count to provide SMS frame synchronization information to the mobile station.

- 20 According to Layer 2 information found in every first slot in each SMS frame, the set of messages in an SMS frame SMS(i) may span a number $M(i)$ of SMS frames before a cycle is completed. Regardless of varying message set cycles among the sub-channels, SMS frame SMS(i) is always followed by SMS frame SMS($(i+1) \bmod N+1$) in order of transmission in this exemplary embodiment. Thus, Layer 3 broadcast SMS messages can span several SMS frames, which represents a tradeoff between the number of slots in each superframe devoted to SMS broadcast and the time needed for message transmission.

THIS PAGE BLANK (USPTO)

-33-

A transition flag (TF) is provided for each SMS sub-channel, and the flags for all SMS sub-channels are submultiplexed onto a single flag, transmitted on the SPACH channel, that points to the next logical SMS frame to be read. For example, FIG. 12 shows flag TF(2) pointing to SMS frame SMS(2). If the transition flag for a sub-channel indicates a change, the mobile station reads an S-BCCH header field at the start of the next logical SMS frame to obtain further information, as described more fully below.

Header information describes the sub-channeling of the broadcast SMS channel and is provided in the first slot of every SMS frame. The mobile can also find the Layer 3 structure of the SMS frame associated with this header. A suitable SMS Header information element located at the start of every SMS frame is shown in the table below.

Information Element	Range (Logical)	Bits
Number of Sub-channels	1-4	2
Sub-channel Number	1-4	2
Phase Length of Sub-ch. Cycle	1-64	6
Phase Number of Sub-ch. Cycle	1-64	6
Number of SMS Messages (N)	1-64 (set to 1 plus value in field)	6
◦ SMS Message ID (Note 1)	0-255 (unique ID in cycle)	8
◦ Layer 2 Frame Start (Note 1)	0-255 (Layer 2 frame identifier)	8

Note 1: N instances of these two elements are sent consecutively.

SMS data may span several SMS frames, but the flags TF enable interruption of the sub-channel cycles (cycle clearing). For example, after a flag TF, the mobile station assumes that the next sub-channel is the start of the new cycle. There are two ways to change the data provided on the broadcast SMS: changing the Layer 3 messages within the SMS (messages may be added and/or

THIS PAGE BLANK (USPTO)

-34-

deleted from any position in the cycle), and changing the structure of the sub-channels.

5 The SMS Message IDs, of which there are a set of 256, and their associated Layer 2 Frame Starts comprise a list of all messages appearing in an SMS frame. SMS Message IDs are unique for each SMS frame and the whole
0 set of 256 values is used before the set begins to be used again in order to aid the mobile in searching for changed message(s) and in avoiding reading messages that have not changed. A Layer 2 Frame Start information element is provided to point to the start of the Layer 2 frame in which the associated SMS message begins (the message does not have to begin at the start of the Layer 2 frame). A description of message delivery is provided in the description of the S-BCCH Layer 2 Protocol given below.

5 In the example shown in the table below, four messages make up SMS frame 1, and it may be assumed that only one slot in each superframe is dedicated to S-BCCH. (Since it is currently preferred that each SMS frame include twenty-four superframes, there are twenty-four slots in each SMS frame.)

THIS PAGE BLANK (USPTO)

-35-

Previous SMS Frame 1 Header				New SMS Frame 1 Header			
5	Number of sub-channels		3	Number of sub-channels		3	
	Sub-channel number		1	Sub-channel number		1	
	Length of sub-ch. cycle		2	Length of sub-ch. cycle		2	
	Phase of sub-ch. cycle		1	Phase of sub-ch. cycle		1	
	Number of SMS messages (N)		4	Number of SMS messages (N)		5	
10	◦1	SMS message ID	1	◦1	SMS message ID	1	
	◦1	Layer 2 Frame Start	1	◦1	Layer 2 Frame Start	1	
	◦2	SMS message ID	2	◦2	SMS message ID	2	
	◦2	Layer 2 Frame Start	2	◦2	Layer 2 Frame Start	2	
	◦3	SMS message ID	3	◦4	SMS message ID	4	
15	◦3	Layer 2 Frame Start	2	◦4	Layer 2 Frame Start	2	
	◦4	SMS message ID	4	◦5	SMS message ID	5	
	◦4	Layer 2 Frame Start	3	◦5	Layer 2 Frame Start	3	
				◦6	SMS message ID	6	
				◦6	Layer 2 Frame Start	3	

In the table above, the mobile is assumed to be monitoring the SPACH when the TF toggles to indicate a change in the S-BCCH. The mobile knows from its own internal superframe count where the start of the SMS frame is, and it can determine that SMS sub-channel three is currently being broadcast by reading the SMS header and that the TF points to a change in SMS sub-channel one. When SMS sub-channel one begins, the mobile reads the SMS header. It determines that message 3 is removed; that the position of message 4 has changed (but the message ID is the same so the mobile does not need to re-read this message); and that new messages 5 and 6 have been added and must be read.

THIS PAGE BLANK (USPTO)

-36-

The mobile may skip the appropriate number of Layer 2 frames to read the new messages.

S-BCCH Layer 2 PROTOCOL

The S-BCCH Layer 2 protocol is used when a TDMA burst carries S-BCCH information. Each S-BCCH Layer 2 protocol frame is constructed to fit in a 125-bit envelope. An additional five bits are reserved for use as tail bits, which are the last bits sent to the channel coder, resulting in a total of 130 bits of Layer 2 information carried within each S-BCCH slot. As noted above, the Layer 2 protocol for S-BCCH operation supports only unacknowledged operation. Several different S-BCCH Layer 2 frames which support this exemplary SMS embodiment are shown in FIGS. 13a, 13b, 13c.

FIG. 13a shows a mandatory minimum S-BCCH BEGIN frame and FIG. 13b shows another S-BCCH BEGIN Frame used when two Layer 3 messages are included in the frame with the second Layer 3 message being continued in a following frame. The BEGIN frames are used for starting the delivery of one or more Layer 3 messages on the S-BCCH, and it is currently preferred that an S-BCCH BEGIN frame be used as the first frame of the S-BCCH cycle. If the first Layer 3 message is shorter than one S-BCCH frame, a begin/end indicator BE is added to the end of the L3DATA field as shown to indicate whether or not an additional Layer 3 message is started within the BEGIN frame. As shown in FIG. 13a, if the BE indicator is set to indicate "END", the rest of the BEGIN frame is padded with FILLER, e.g., zeroes. As shown in FIG. 13b, if the BE indicator is set to indicate "BEGIN", a new Layer 3 message is started in the BEGIN frame. If the L3DATA field ends on an S-BCCH frame boundary, the BE indicator is not included in the frame; an "END" indication is implied. If the L3DATA field ends with less than nine bits remaining in the S-BCCH frame, the BE indicator is set to "END", and the rest of the frame is padded with FILLER.

THIS PAGE BLANK (USPTO)

-37-

FIG. 13c shows an S-BCCH CONTINUE Frame (mandatory minimum), which is used for continuation of a Layer 3 message that was too long to fit into the previous frame. The continuation length indicator CLI field indicates how many bits of the CONTINUE frame belong to the continued message, and thus the preceding Layer 3 message may have to be padded with FILLER. If the BE indicator is set to "END", the rest of the CONTINUE frame is padded with FILLER. If the BE indicator is set to "BEGIN", a new Layer 3 message is started in the CONTINUE frame. If the L3DATA field ends on an S-BCCH frame boundary, the BE indicator is not included in the frame; an "END" indication is implied. If the L3DATA field ends with less than nine bits remaining in the S-BCCH frame, the BE indicator is set to "END", and the rest of the frame is padded with FILLER.

The CLI makes it possible for mobile stations to receive any message starting in a continuation frame, even if the preceding logical frame was not received. The following table summarizes the fields included in the S-BCCH Layer 2 protocol frames.

THIS PAGE BLANK (USPTO)

-38-

Field Name	Bit Length	Values
SCS = S-BCCH Cycle Start	1	0 = Not the start of an S-BCCH cycle 1 = Start of an S-BCCH cycle
BC = Begin / Continue	1	0 = Begin 1 = Continue
CLI = Continuation Length Indicator	7	Number of bits remaining in previous Layer 3 message.
L3LI = Layer 3 Length Indicator	8	Variable length Layer 3 messages supported up to a maximum of 255 octets
L3DATA = Layer 3 Data	Variable	Contains a portion (some or all) of the Layer 3 message having an overall length indicated by L3LI. The portion of this field not used to carry Layer 3 data is filled with zeroes.
BE = Begin / End	1	0 = Beginning 1 = End
FILLER = Burst Filler	Variable	All filler bits are set zero
CRC = Cyclic Redundancy Code	16	Same generator polynomial as IS-54B. The nominal DVCC is applied in the calculation of CRC for each S-BCCH Layer 2 frame.

10

Similar logical frames can be defined for the F-BCCH and E-BCCH, as described in U.S. Patent Application No. 08/147,254 for example, but these are beyond the scope of this application.

THIS PAGE BLANK (USPTO)

Layer 3 MESSAGES

The S-BCCH Layer 3 messages that are mapped to the Layer 2 frames are described below. In all messages shown in tabular form below, the information elements in the top rows of the tables are preferably the first elements to be delivered to Layer 2. In the information elements, the most significant bit (the left-most bit in the tables) is the first bit to be delivered to Layer 2. The information elements are described in alphabetical order after the description of the messages below.

There are two types of S-BCCH messages used for SMS broadcast: SMS frame header messages; and SMS non-header messages, which are those used to transfer the actual messages to the mobile stations.

The SMS frame header messages describe the structure of the SMS sub-channel, and are provided in the first slot of each SMS frame. The format of a suitable SMS frame header message is described in the following table.

Information Element	Type	Bit Length
Message Type	M	8
Number of Sub-channels	M	2
Sub-channel Number	M	2
Phase Length of Sub-ch. Cycle	M	6
Phase Number of Sub-ch. Cycle	M	6
Number of SMS Messages (N)	M	6
◦ SMS Message ID (Note 1)	M	8
◦ Layer 2 Frame Start (Note 1)	M	8
		Total = 46

NOTE 1: N instances of these two elements are sent consecutively.

The format of a suitable SMS non-header, broadcast message is as follows:

THIS PAGE BLANK (USPTO)

-40-

Information Element	Type	Bit Length
Message Type	M	8
SMS Message ID	M	8
Text Message Data Unit	M	N*8 N max. = 253

5 In one aspect of Applicants' invention, SMS messages may be encrypted
in a way that supports different classes of message service, much like cable
television systems distinguish premium classes of service from a basic service
class by scrambling or otherwise protecting the premium programming. For
example, three classes might be provided as follows: a basic class in which any
10 subscriber paying an appropriate fee would be able to de-crypt some of the SMS
broadcast messages, such as product advertisements, weather and vehicle traffic
announcements; a higher class in which a subscriber paying a higher fee would
be able to de-crypt the SMS broadcast messages available to the basic class and
additional messages, such as news items; and a highest class in which a
15 subscriber paying a highest fee would be able to de-crypt all of the SMS
broadcast messages, including financial quotations and higher-value items of
information.

The de-cryption of the SMS messages could be carried out by the
processing units in the mobile stations according to any of a wide variety of
20 cryptographic techniques. Preferably, each broadcast message would include as
an attribute an indicator for determining which encryption key or algorithm
should be used to decode the respective message. Such attributes might be
included in the SMS frame headers, and the encryption keys or algorithms could
be sent to the mobiles over the air or entered directly, via a "smart card", for
25 example. As an alternative, the sub-channels could be individually encrypted, so
that broadcast SMS messages included in the time slots of one of the SMS sub-
channels are encrypted according to one encryption method and the broadcast

THIS PAGE BLANK (USPTO)

-41-

SMS messages included in the time slots of another SMS sub-channel are encrypted according to a another encryption method.

INFORMATION ELEMENT DESCRIPTION

- 5 A few coding rules apply to the information element descriptions. For example, information elements of the type "flag" have values of 0 to indicate "disable", or "off", or "false", and values of 1 to indicate "enable", or "on", or "true". Also, certain BCCH fields do NOT trigger a transition in the BCCH change flag in the SPACH; those fields are designated as non-critical, or "NC".
- 10 Information elements of the type "transition" are modulo-1 counters for indicating changes in current status. The channel number is coded in accordance with the IS-54B standard, unless otherwise noted. All lengths are specified in bits, unless otherwise noted.

Layer 2 Frame Start

- 15 This variable indicates the number of slots from the start of the SMS sub-channel cycle to the beginning of the SMS message, which may not begin in the indicated SMS slot but may be contained in an end/begin burst used to start delivery of this message.

THIS PAGE BLANK (USPTO)

-42-

Message Type

This 8-bit information element identifies the function of the message being sent. The message types are coded as follows:

S-BCCH Messages	Code (binary-hex)
5 Broadcast Information Message	0010 0111 - 27

Number of SMS Messages

This variable indicates the number of broadcast SMS messages in this SMS frame (1 plus the value in this field).

Number of Sub-channels

- 10 This variable indicates the number of SMS sub-channels being used by this DCCH (1 plus the value in this field).

Phase Length of Sub-ch. Cycle

This variable indicates the number of SMS frames that make up one cycle (1 plus the value in this field).

- 15 Phase Number of Sub-ch. Cycle

This variable indicates which SMS frame in the cycle is currently being broadcast.

Sub-channel Number

- 20 This variable indicates which sub-channel is currently being broadcast.
- 25 According to another exemplary embodiment, the amount of bandwidth per sub-channel (i.e., the periodicity at which each sub-channel is transmitted) and the ordering of sub-channels is dynamic to provide additional flexibility to broadcast SMS systems. Although the term "sub-channels" is used herein, those skilled in the art will appreciate that any other term or phrase which connotes logical grouping of SMS messages could be used to describe these groupings of the present invention. Moreover, according to this exemplary embodiment, a greater number of SMS sub-channels, e.g., 8, 16, 32, 64, etc., can be supported than the four sub-channels used to illustrate the previous exemplary embodiment.

THIS PAGE BLANK (USPTO)

-43-

For the purposes of illustration, rather than limitation, an example will be provided wherein up to 32 S-BCCH sub-channels are supported.

According to this exemplary embodiment, a particular subset of message attributes is associated with each sub-channel rather than broadcasting messages having any set of attributes on any sub-channel, as in the previous exemplary embodiment. The particular order in (and periodicity at) which these sub-channels are transmitted can be varied by the system operator according to, for example, the number of messages which have the attribute(s) associated with each sub-channel. The system can broadcast messages using associated with a sub-channel on, for example, a number of contiguous S-BCCH time slots, which number may vary for each sub-channel. The broadcasting of a sub-channel may, however, be interrupted by the system in order to broadcast messages on sub-channels 0 and 1 for reasons that will become apparent.

Since sub-channeling according to this exemplary embodiment does not have a fixed, time multiplexed format such as that provided in the earlier embodiment, a different mechanism (i.e., other than an SMS frame header) is used to provide overhead information. In this example overhead information including, for example, the total number of sub-channels currently activated, the message encryption algorithm associated with each sub-channel (if any), the user group associated with each sub-channel (if any), and other S-BCCH attributes described below, is provided on sub-channel 0. Channel 0 is dedicated to this overhead function so that mobile stations will know where to find this information. When a cycle of sub-channel 0 information is to be sent by the system (e.g., broadcast from a base station), it can be started in a first S-BCCH time slot coincident with a hyperframe counter value of zero. For example, sub-channel 0 can be broadcast at least once every $12 \cdot N$ hyperframes ($N=1,2,3,\dots$) or when otherwise desired by a system operator. Once started, the broadcast of sub-channel 0 should be completed without interruption using consecutive S-BCCH time slots.

THIS PAGE BLANK (USPTO)

-44-

Sub-channel 1 is dedicated, according to this exemplary embodiment, to the provision of messages associated with other sub-channels (i.e., sub-channels 2-31 in this example) that have recently been changed or added. Typically, deleted messages are of no interest to mobile stations, however, those skilled in the art will recognize that the present invention can be readily extended to provide an indication to mobile units that a message has been deleted in a manner similar to that described herein for changed messages and added messages. The broadcast of sub-channel 1 by the system may commence after the completion of any sub-channel or by interrupting a sub-channel (other than sub-channels 0 or 1). For example, it may be considered desirable by a system operator to begin increase the periodicity of transmission of sub-channel 1 after the transmission of sub-channel 0 in which a change or changes have been indicated. Once the broadcast of sub-channel 1 has begun, it should be completed without interruption using consecutive S-BCCH time slots. By reading sub-channel 1, a mobile station will be able to quickly access changed or added messages of interest.

From the mobile station's perspective, upon camping on a DCCH the mobile can, for example, read sub-channel 0 to determine if it needs to acquire the S-BCCH information broadcast thereon that is associated with that particular DCCH. For example, after cell reselection, the mobile may have camped on a DCCH whose S-BCCH has a different structure in terms of the number of sub-channels currently activated, the user groups and/or encryption techniques associated with each sub-channel, etc. In such a case, the mobile would need this information in order to perform additional SMS activities supported by that DCCH. The selective acquisition of S-BCCH information is supported by, for example, a broadcast domain indicator provided as part of a Layer 3 message transmitted on sub-channel 0. This broadcast domain indicator is discussed in more detail below. For example, a mobile station reading sub-channel 0 may determine that it has locked to a DCCH associated with the same broadcast domain under which that mobile was previously operating, i.e., if the broadcast

THIS PAGE BLANK (USPTO)

-45-

domain value read by the mobile station is the same as that previously read and stored, but where some changes have occurred in the S-BCCH information. In such a situation, the mobile station may need to read only the S-BCCH information which has changed since certain sub-channeling structure will be common to cells which support the same broadcast domain. More detailed examples describing of the interaction between a mobile station reading sub-channel 0 and the broadcast domain indicator will be provided after a description of the Layer 2 protocols and Layer 3 messages.

While in the process of acquiring the S-BCCH information broadcast on sub-channel 0, this information could be changed by the system, e.g., to add a new sub-channel to handle messages sent to a new user group and/or using a different encryption algorithm. Similarly, the S-BCCH information associated with a DCCH can change after it is acquired by a mobile station. In either case a Layer 2 change indication is sent to the mobile which responds by reading sub-channel 0. For example, a change notification bit can be placed in the SPACH header and used to notify mobile stations of changes in the content of the S-BCCH information. For a detailed description of the SPACH and SPACH header, the interested reader is referred to U.S. Patent Application Serial No. 08/331,816 entitled "Layer 2 Protocol in Cellular Communication System" filed on October 31, 1994, which disclosure is incorporated here by reference.

According to this exemplary embodiment, and as distinguished from the transition flags TF(i), change indication is generic in the sense that the particular sub-channel or sub-channels which have been modified are not identified in the Layer 2 change notification. Instead, the affected mobile stations will read sub-channel 0 to determine the specific sub-channel or sub-channels which have been modified. In this way the modified S-BCCH information can be sent to the mobile stations beginning in the hyperframe immediately following the hyperframe in which the Layer 2 change indication is provided.

The exemplary Layer 2 protocol defined below supports S-BCCH operation to allow a mobile station to uniquely determine the start and end of a

THIS PAGE BLANK (USPTO)

-46-

sub-channel and to begin reading a sub-channel starting with any Layer 2 frame belonging to that sub-channel. According to this exemplary embodiment, each sub-channel is sent using up to 256 Layer 2 frames. Of course, those skilled in the art will appreciate that other sub-channel capacities can be used without departing from the spirit of the present invention. An exemplary 256 Layer 2 frame sub-channel would, however, provide about 10 maximum length (i.e., 255 octets) Layer 3 messages per sub-channel or about 25 SMS messages per S-BCCH sub-channel assuming an average of 100 octets of data per message. In this exemplary embodiment, a Layer 3 message qualifier can be used to identify up to, for example, 256 distinct S-BCCH Payload messages over all of the SMS "traffic" sub-channels 2-31. Additional S-BCCH messages can be identified by creating other types of Layer 3 messages and pairing the associated Layer 3 message type with the Layer 3 message qualifier e.g., 256 different S-BCCH messages per pair. Having provided an overview of message delivery in accordance with this second exemplary SMS embodiment, exemplary Layer 2 and Layer 3 protocols for supporting these functions will now be described.

S-BCCH LAYER 2 PROTOCOL (Second Exemplary Embodiment)

The S-BCCH Layer 2 protocol is used when a TDMA slot is used to carry S-BCCH information. The S-BCCH protocol allows for supporting up to a maximum of 32 distinct S-BCCH sub-channels. The set of layer 3 messages comprising a S-BCCH sub-channel is sent using up to 256 S-BCCH layer 2 protocol frames.

Each S-BCCH Layer 2 protocol frame can be constructed to fit within a 125 bit envelope. An additional 5 bits are reserved for use as tail bits resulting in a total of 130 bits of information carried within each S-BCCH slot. The Layer 2 protocol defined in this exemplary embodiment for S-BCCH operation supports only unacknowledged operation. Figures 14(a)-14(e) provide examples of Layer 2 S-BCCH frames.

THIS PAGE BLANK (USPTO)

-47-

The BEGIN frame is used for starting the delivery of one or more Layer 3 messages on any given sub-channel of the S-BCCH. The Layer 3 that constitutes the opening message of a full cycle of S-BCCH information for any sub-channel shall be transmitted starting with a BEGIN FRAME and shall occupy the first L3DATA field included in the BEGIN frame should more than one L3DATA field be present therein. Exemplary rules for the placement of Layer 3 messages within a BEGIN frame are as follows.

If a Layer 3 message fits entirely within the L3DATA field of a BEGIN frame with 9 or more bits remaining in the frame, the Begin Indicator (BI) is included immediately after the L3DATA field to indicate whether or not an additional Layer 3 message is started within the frame. If BI=0, no other Layer 3 message is started and the rest of the frame is padded with FILLER. If BI=1 a L3LI field is included immediately after the BI field. The L3LI field is then followed by another L3DATA field containing a portion of the new Layer 3 message determined by the number of bits remaining in the frame.

If, on the other hand, a Layer 3 message fits entirely within the L3DATA field of a BEGIN frame with from 1 to 8 bits remaining in the frame and another Layer 3 message is to be sent, BI=0 is included immediately after the L3DATA field. The rest of the frame is then padded with FILLER and the next Layer 3 message is sent starting with another BEGIN frame. If a Layer 3 message fits entirely within the L3DATA field of a BEGIN frame with from 1 to 8 bits remaining in the frame and no other Layer 3 message is to be sent, BI=0 is included immediately after the L3DATA field and the rest of the frame is padded with FILLER. If a Layer 3 message fits entirely within the L3DATA field of a BEGIN frame with no bits remaining, the BI field is not present and the end of the Layer 3 message is implied. This case is exemplified in Figure 14a.

Lastly, if a Layer 3 message does not fit entirely within the L3DATA field of a BEGIN frame, it is completed using as many CONTINUE frames as necessary. The other fields illustrated in FIG. 14a are described in Table 1 below.

THIS PAGE BLANK (USPTO)

-48-

The CONTINUE frame is used whenever a Layer 3 message cannot be completed within the previous S-BCCH Layer 2 frame. Exemplary CONTINUE frames are illustrated in FIGS. 14b-14d. The CLI field indicates how many bits of the CONTINUE frame belong to the continued Layer 3 message. This in turn allows for mobile stations to receive a portion of a new message which may be present in the CONTINUE frame following the L3DATA field used to complete a message continued from the previous frame. Exemplary rules for the placement of Layer 3 message information within a CONTINUE frame are as follows.

10 If the CLI field indicates that the remainder of a continued Layer 3 message fits entirely within the CONTINUE frame with 9 or more bits remaining in the frame, the Begin Indicator (BI) is included immediately after the L3DATA field to indicate whether or not an additional Layer 3 message is started within the frame. For example, if BI=0 no other Layer 3 message is started and the rest of the frame is padded with FILLER. This case is illustrated as FIG. 14b.

15 If BI=1, then an L3LI field is included immediately after the BI field. The L3LI field is then followed by another L3DATA field containing a portion of the new Layer 3 message. The length of the portion of the new Layer 3 message in the second L3DATA field is determined by the number of bits remaining in the frame. This case is illustrated in FIG. 14c.

20

 If CLI indicates that the remainder of a continued Layer 3 message fits entirely within the CONTINUE frame with from 1 to 8 bits remaining in the frame and another Layer 3 message is to be sent, BI=0 is included immediately after the L3DATA field. The rest of the frame is padded with FILLER and the next Layer 3 message is sent starting with another BEGIN frame. This case is also exemplified by the format of FIG. 14b.

25

 If CLI indicates that the remainder of a continued Layer 3 message fits entirely within the CONTINUE frame with from 1 to 8 bits remaining in the frame and no other Layer 3 message is to be sent, BI=0 is included immediately after the L3DATA and the rest of the frame is padded with FILLER. If CLI

30

THIS PAGE BLANK (USPTO)

indicates that the entire CONTINUE frame contains information belonging to a continued Layer 3 message, the BI field is not present in the frame. This is illustrated in FIG. 14d.

- 5 A continued Layer 3 message is completed using as many CONTINUE frames as necessary. The following table summarizes the exemplary fields provided in these S-BCCH Layer 2 frames according to this exemplary embodiment.

TABLE 1: S-BCCH Layer 2 Protocol Field Summary

	FIELD NAME	LENGTH (Bits)	VALUES
10	BC=Begin/Continue	1	Identifies the type of L2 frame (0=Begin, 1=Continue)
	SID=Sub-channel ID	5	Uniquely identifies the sub-channel that a L2 frame belongs to (0..31).
	FDC=Frame Down Counter	8	Uniquely identifies a Layer 2 frame used in sending a cycle of sub-channel information (0..255).
15	SSI=Sub-channel Start Indicator	1	Indicates whether or not a L2 frame is the first frame used in sending a cycle of sub-channel information (0=No, 1=Yes).
	SCN=S-BCCH Change Notification	1	Transitions whenever there is a change in the content of S-BCCH information. A mobile station responds by reading S-BCCH information on sub-channel 0.
	CLI=Continuation Length Indicator	7	Number of bits in the current L2 frame used to carry information from a previously initiated L3 message.

THIS PAGE BLANK (USPTO)

-50-

FIELD NAME	LENGTH (Bits)	VALUES
L3LI=Layer 3 Length indicator	8	Variable length Layer 3 messages supported from 0 up to a maximum of 255 octets.
L3DATA=Layer 3 Data	Variable	Contains a portion (some or all) of the Layer 3 message having an overall length as indicated by L3LI. The portion of this field not used to carry Layer 3 information is filled with zeros.
BI=Begin Indicator	1	0=No additional Layer 3 message present 1=Additional Layer 3 message present
5 FILLER=Burst Filler	Variable	All filler bits are set to zero.
CRC=Cycle Redundancy Code	16	Same generator polynomial as IS-54B. The nominal DVCC is applied in the calculation of CRC for each S-BCCH Layer 2 frame.

- An S-BCCH Request primitive can be provided to transfer Layer 3 messages to be sent on the S-BCCH to Layer 2. For example, the S-BCCH Request primitive can include the following protocol elements:
- (1) a Layer 3 message (examples below);
 - (2) a Layer 3 Length Indicator (L3LI) providing the length of the Layer 3 message (e.g., in octets); and
 - (3) a sub-channel ID which identifies the sub-channel that the Layer 3 message is associated with.

LAYER 3 MESSAGES (Second Exemplary Embodiment)

Exemplary Layer 3 messages which can be mapped to Layer 2, e.g., using the primitive described above are set forth below. As in the description of

THIS PAGE BLANK (USPTO)

-51-

the previous exemplary embodiment, the information elements in the top rows of tables can be the first elements delivered to Layer 2. In the information elements, the most significant (i.e., leftmost) bit is the first bit to be delivered to Layer 2. The information elements are described in alphabetical order after the description of the message below.

A **Sub-channel Configuration** message is sent on sub-channel 0 to define the format of supported channels. An exemplary format for the **Sub-channel Configuration** message is illustrated below.

Information Element	Reference	Type	Length
Protocol Discriminator		M	2
Message Type		M	6
Sub-channel Count (N)		M	5
Sub-channel Info (Note 1)		O	13-*

Note 1: N instances of this information element are included up to a maximum number of supported "traffic" subchannels, e.g., 30.

The **Sub-channel Count** information element identifies the number of sub-channels used in support of sending S-BCCH information. In this exemplary embodiment five bits are provided to support the 32 sub-channels. Of course more or fewer bits could be provided to represent this value if more or fewer sub-channels are to be supported, respectively.

The **Sub-Channel Info** information element identifies the attributes of supported S-BCCH sub-channels. An exemplary format for this information element is shown below.

THIS PAGE BLANK (USPTO)

-52-

Field	Length
Sub-channel ID (Note 1)	5
MEA	3
MEK	3
Wildcard Indicator	1
Broadcast Mode	1
User Group Type (Note 2)	0,2
User Group ID (Note 2)	0,20,24,34 or 50

5

10

Note 1: Sub-channels 0 and 1 are defined implicitly and therefore need not be explicitly defined.

Note 2: Only present if the Broadcast Mode indicates User Group ID specific broadcast.

Each of the fields of the Sub-channel Info information element and the attributes which they describe are set forth in more detail below.

15

The Sub-channel ID field identifies a specific S-BCCH sub-channel (0..31) associated with each of the other parameters in the information element. This field can be used by a mobile station as an index by which the mobile station can update its information as to the structure of certain sub-channels as needed, e.g., newly added sub-channels.

20

The MEA and MEK fields identify the encryption technique (if any) associated with the particular sub-channel identified by the sub-channel ID field. Encryption can, for example, be one of the message attributes upon which the grouping of messages into logical sub-channels can be based. The MEA field can, for example, be coded as follows.

100

-53-

Value	Function
000	No Message Encryption
001	Message Encryption Algorithm A
All other values are reserved	

5 The MEK field can, for example, be coded as follows.

Value	Function
001	Message Encryption Key A
All other values are reserved	

10 The combination of both an MEA and MEK can be used to provide, for example, different levels of service to publicly available channels. For example, different encryption algorithms could be associated with each encryption key to provide different levels of access to information. Thus, a Bronze class message group could be associated with a first encryption algorithm and an encryption key, a Silver class message group (i.e., sub-channel) could be associated with a second encryption algorithm and that encryption key, and a Gold class message group could be associated with a third encryption algorithm and that encryption key.

15 The Wildcard Indicator field indicates whether or not the sub-channel identified by the sub-channel ID field belongs to the broadcast domain. Each broadcast domain (e.g., each system operator) may have certain standard or common sub-channels. Other sub-channels, which are not common to a broadcast domain, may nonetheless be broadcast by the system. The mobile station learns of these non-standard sub-channels by reading the Wildcard Indicator. The Wildcard Indicator field can, for example, be coded as follows.

THIS PAGE BLANK (USPTO)

-54-

Value	Function
0	Standard Sub-channel (part of Broadcast Domain)
1	Wildcard Sub-channel (not part of Broadcast Domain)

5 The Broadcast Mode field indicates whether or not the sub-channel identified in sub-channel ID field is restricted to a particular user group. The Broadcast Mode field can, for example, be coded as follows.

Value	Function
0	Unrestricted Broadcast
1	User Group ID Specific Broadcast

10 The User Group Type and User Group ID fields specify the user group to which this sub-channel is restricted if the appropriate value is set in the Broadcast Mode field. The User Group Type field can, for example, be coded as follows.

15

Value	Function
00	20-bit Local UGID
01	24-bit SOC UGID
10	34-bit National UGID
11	50-bit International UGID

20 The User Group Type field indicates, for example, how many bits to expect in the User Group ID field, which identifies the User Group to which an S-BCCH sub-channel has been allocated.

THIS PAGE BLANK (USPTO)

-55-

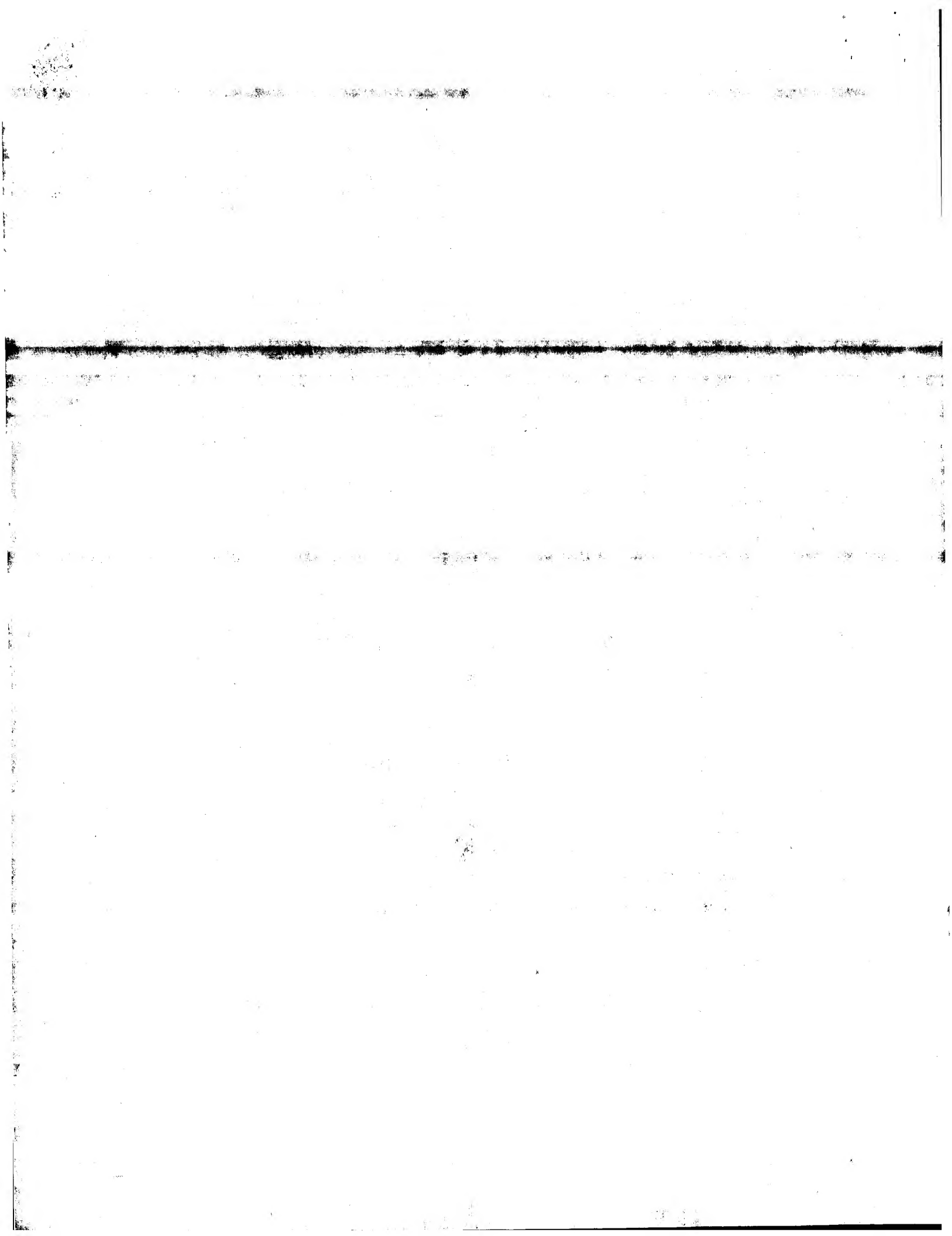
The **Sub-channel Change Summary** message is also sent on S-BCCH sub-channel 0 to indicate the nature of changes made to S-BCCH information. An exemplary format for this message is set forth below.

Information Element	Reference	Type	Length
Protocol Discriminator		M	2
Message Type		M	6
Broadcast Domain ID		M	8
Change Indicator Map		M	32
Change Acquisition Map		M	32

The **Broadcast Domain ID** information element is used to identify, for example, a system operator code (SOC) specific S-BCCH broadcast area as described above. More specifically, the **Broadcast Domain ID** provides an indication to a mobile station of whether certain commonalities expected within a broadcast domain are available to that mobile station when the mobile station locks on to another DCCH. For example, adjacent DCCHs that have the same SOC and that send the same set of S-BCCH information on the same standard sub-channels shall use the same **Broadcast Domain ID** value.

The **Change Indicator Map** information element is used to provide change indication information on a per sub-channel basis. The leftmost bit in this map corresponds to sub-channel 31 and the rightmost bit corresponds to sub-channel 0. Whenever there is a modification to the content of a sub-channel (other than a deletion) the corresponding bit position in this map is toggled. Mobile stations need only proceed to acquire the new S-BCCH information for the modified sub-channels that are of interest, e.g., according to the **Change Acquisition Map** element described below.

The **Change Acquisition Map** information element is use to provide change acquisition information on a per sub-channel basis. The leftmost bit in



-56-

this map corresponds to sub-channel 31 and the rightmost bit corresponds to sub-channel 0. Whenever there is a modification to the content of a sub-channel (other than a deletion) the corresponding bit position in this map is used to inform mobile stations how to acquire the new information as follows. When a bit of this map is set to 0, then mobile stations that have previously read the newly modified sub-channel associated with that bit shall acquire the new information by reading sub-channel 1. Mobile stations that are in the process of reading or have never read the newly modified sub-channel shall acquire the new information by (re-)reading a full cycle of information from the modified sub-channel. When a bit of this map is set to 1, mobile stations shall acquire the new information by reading a full cycle of information from the newly modified sub-channel.

The S-BCCH Payload message is sent on sub-channels 1 through 31 in order to provide the Layer 3 messages specific to S-BCCH operation and can, for example, have the following format.

Information Element	Reference	Type	Length
Protocol Discriminator		M	2
Message Type		M	6
Message Type Qualifier		M	8
Other Data (TBD)		TBD	TBD

The Message Type information element identifies the function of the message, e.g., an S-BCCH Payload message. The Message Type Qualifier information element is used to identify up to 256 distinct S-BCCH messages. For example:

THIS PAGE BLANK (USPTO)

-57-

5

Value	Function
0000 0000	Casino Clips
0000 0001	Road Report
0000 0010	Rugby News
All other values are reserved.	

The **Other Data (TBD)** field can be used to provide, e.g., higher layer protocols such as how long a message should be retained for retransmission on a sub-channel.

10

The **Sub-channel Delimiter** message can be sent on sub-channel 1 to delimit groups of S-BCCH Payload messages, also sent on sub-channel 1, that are associated with specific sub-channels. This allows mobile stations to determine the nominal sub-channels that each S-BCCH Payload message is associated with. The **Sub-channel Delimiter** message can, for example, have the following format.

15

Information Element	Reference	Type	Length
Protocol Discriminator		M	2
Message Type		M	6
Sub-channel ID		M	5

20

Having described exemplary Layer 3 messages, the operation of a mobile station in such a system will now be described by way of several examples. As mentioned above, a mobile station that acquires a new DCCH (e.g., by cell reselection) shall perform an S-BCCH update by first reading sub-channel 0 to determine if the S-BCCH information associated with this DCCH is different.

25

For example, assume that the mobile station has travelled to a cell whose DCCH is associated with another broadcast domain (e.g., a different system operator).

THIS PAGE BLANK (USPTO)

-58-

Under these circumstances, the mobile station will read a full cycle of information on all sub-channels determined to be of interest according to subchannel 0 information. Sub-channels of interest can, for example, include those sub-channels whose encryption techniques match those which the mobile station can decrypt and/or those sub-channels accessible to a common user group supported by the mobile station.

As another example, consider a mobile station which is informed, by a change in the notification flag found in the SPACH header, that the contents of the S-BCCH have changed. Suppose, for this example, that the change constitutes the addition of a new sub-channel. The mobile station will then read sub-channel 0. If it first receives a Subchannel Change Summary message, the mobile station will learn, from the setting of a bit in the Change Indicator Map information element, that a new sub-channel has been added. However, the mobile station will not know, based on this message, whether or not this is a sub-channel of interest, since the Subchannel Change Summary message does not provide an indication of the sub-channel attributes associated with the newly added sub-channel. Accordingly, the mobile will read a Subchannel configuration message to determine if it is interested in the new sub-channel and read a cycle of that sub-channel as desired.

As another example, consider a mobile station that is informed of a change in S-BCCH information via the S-BCCH change notification flag carried in the SPACH header. Suppose, for this example, that the change constitutes the modification of a single message sent on a specific sub-channel of interest to the mobile station. The mobile station responds to the change notification by first reading sub-channel 0 to acquire the Sub-channel Change Summary message. The Change Indicator Map information element contained within this message identifies that only a single sub-channel has changed. A bit position in the Change Indicator Map information element and its corresponding value serves to uniquely identify the changed sub-channel. The Change Acquisition Map information element, also contained within this message, indicates how the

THIS PAGE BLANK (USPTO)

-59-

changed information is to be acquired for the changed sub-channel identified. For this example, assume that the bit position in the **Change Acquisition Map** information element corresponding to the changed sub-channel indicates that sub-channel 1 should be read to acquire the changes associated with the changed sub-channel. The mobile station then proceeds to read a full set of information sent on sub-channel 1 (in this example only a single S-BCCH Payload message since only one sub-channel has changed) and updates its S-BCCH information accordingly.

Although the present invention has been described in terms of attributes such as types of encryption and user group assignment, those skilled in the art will appreciate that other types of attributes can be added or substituted for those described herein. Moreover, other broadcast SMS embodiments will also be apparent to those skilled in the art as being within the scope of the present invention without a detailed description thereof. For example, sub-channel 1 need not be dedicated to carry change information. Instead, additional segmentation can be provided at Layer 2 whereby strings of Layer 2 frames are also defined to allow guaranteed delivery of these distinct strings without interruption (unless aborted) while still allowing for a fast real time response to information change situations.

Another technique would be to provide only a single (large) payload sub-channel used for carrying the full set of broadcast information rather than the exemplary sub-channels 2...32 described above. Changes could still be carried on sub-channel 1 and sub-channel 0 could still contain sub-channel structure and detailed change indication information. Message encryption and user group operation would then be specified on a per BCCH message basis.

Moreover, although these illustrative embodiments describe a mobile station that first reads sub-channel 0 upon receiving a change notification, those skilled in the art will appreciate that the mobile station could vary this procedure. For example, sub-channel 1 could be read first by the mobile station to determine which messages have changed. A change flag could be provided on sub-channel

THIS PAGE BLANK (USPTO)

-60-

1 to indicate whether or the information on sub-channel 0 has changed, at which point the mobile station could then acquire the S-BCCH information of sub-channel 0.

5 It is, of course, possible to embody the invention in specific forms other than those described above without departing from the spirit of the invention. The embodiments described above are merely illustrative and should not be considered restrictive in any way. The scope of the invention is determined by the following claims, rather than the preceding description, and all variations and
10 equivalents which fall within the scope of the claims are intended to be embraced therein.

THIS PAGE BLANK (USPTO)

-61-

WHAT IS CLAIMED IS:

1. A method of communicating information to a remote station comprising the steps of:
 - grouping the information into a plurality of successive time slots on a
 - 5 radio carrier signal;
 - grouping the time slots into a plurality of successive superframes; and
 - grouping the successive superframes into a plurality of successive hyperframes, wherein at least two successive superframes are grouped into each hyperframe;
 - 10 wherein each superframe includes time slots comprising a logical channel for broadcast control information and time slots comprising a logical paging channel, and the broadcast control information comprises special messages that are included in respective time slots comprising a logical special message channel.
- 15 2. The method of claim 1, wherein the time slots of the special message channel are grouped in successive SMS frames, and the SMS frames are synchronized with respective hyperframes.
3. The method of claim 2, wherein each SMS frame corresponds to a respective one of a plurality of SMS sub-channels.
- 20 4. The method of claim 3, wherein a special message spans at least two SMS frames of a respective SMS sub-channel.
5. The method of claim 3, wherein the special messages included in the time slots of a first one of the SMS sub-channels are encrypted according to a first encryption method and the special messages included in the time slots of at
- 25 least one other SMS sub-channel are encrypted according to another encryption method.
6. The method of claim 3, wherein each special message is encrypted according to a respective encryption method.

THIS PAGE BLANK (USPTO)

-62-

7. A method for transmitting messages in a radiocommunication system, comprising the steps of:

- identifying a plurality of attributes associated with said messages;
- selecting subsets of said attributes;
- 5 grouping said messages using said selected subsets and at least one attribute associated with each message; and
- selectively transmitting said groups of messages.

8. The method for transmitting messages of claim 8, wherein said step of identifying further comprises:

- 10 identifying a plurality of encryption techniques and a plurality of user groups as said plurality of attributes.

9. The method for transmitting messages of claim 8, wherein said steps of selecting subsets and grouping messages further comprise:

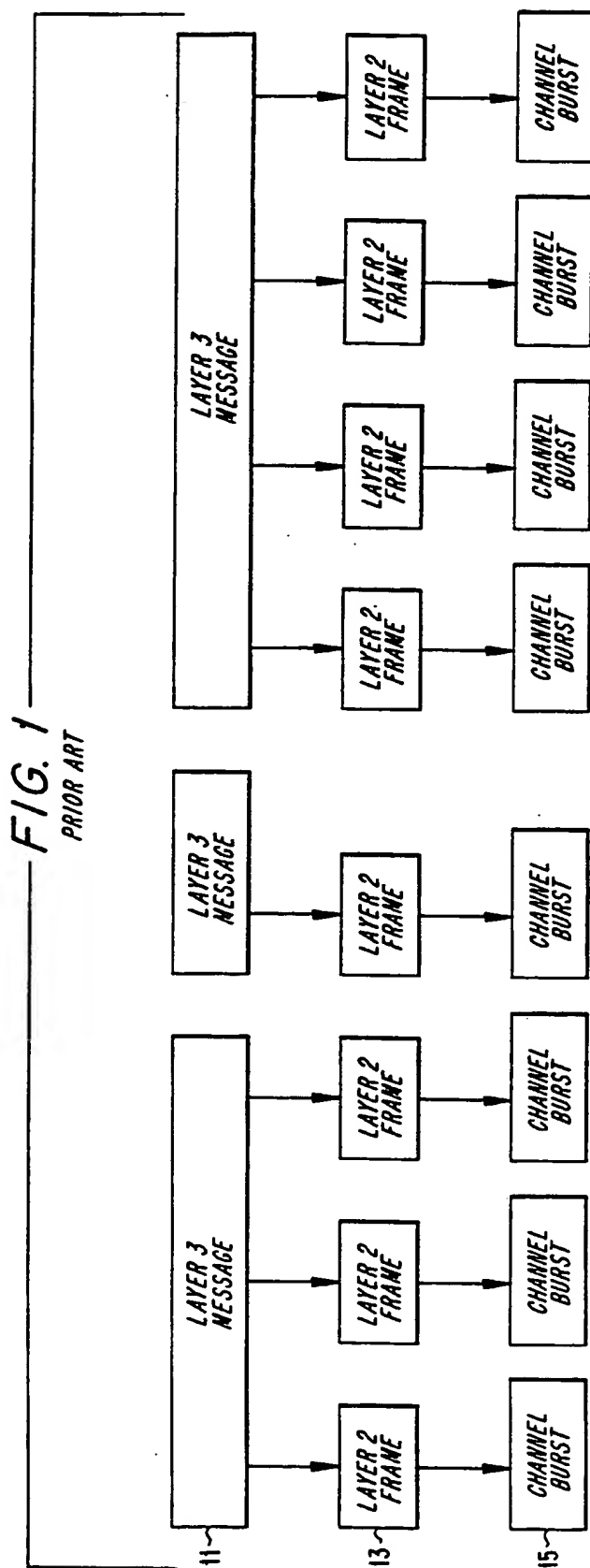
- 15 selecting a subset including a first one of said plurality of encryption techniques; and
- grouping together messages having as said at least one attribute said first one of said plurality of encryption techniques.

10. The method for transmitting messages of claim 8, wherein said steps of selecting subsets and grouping messages further comprise:

- 20 selecting a subset including a first one of said plurality of user groups; and
- grouping together messages having as said at least one attribute a user group identification associated with said first one of said plurality of user groups.

THIS PAGE BLANK (USPTO)

1/10



THIS PAGE BLANK (USPTO)

2/10

FIG. 2

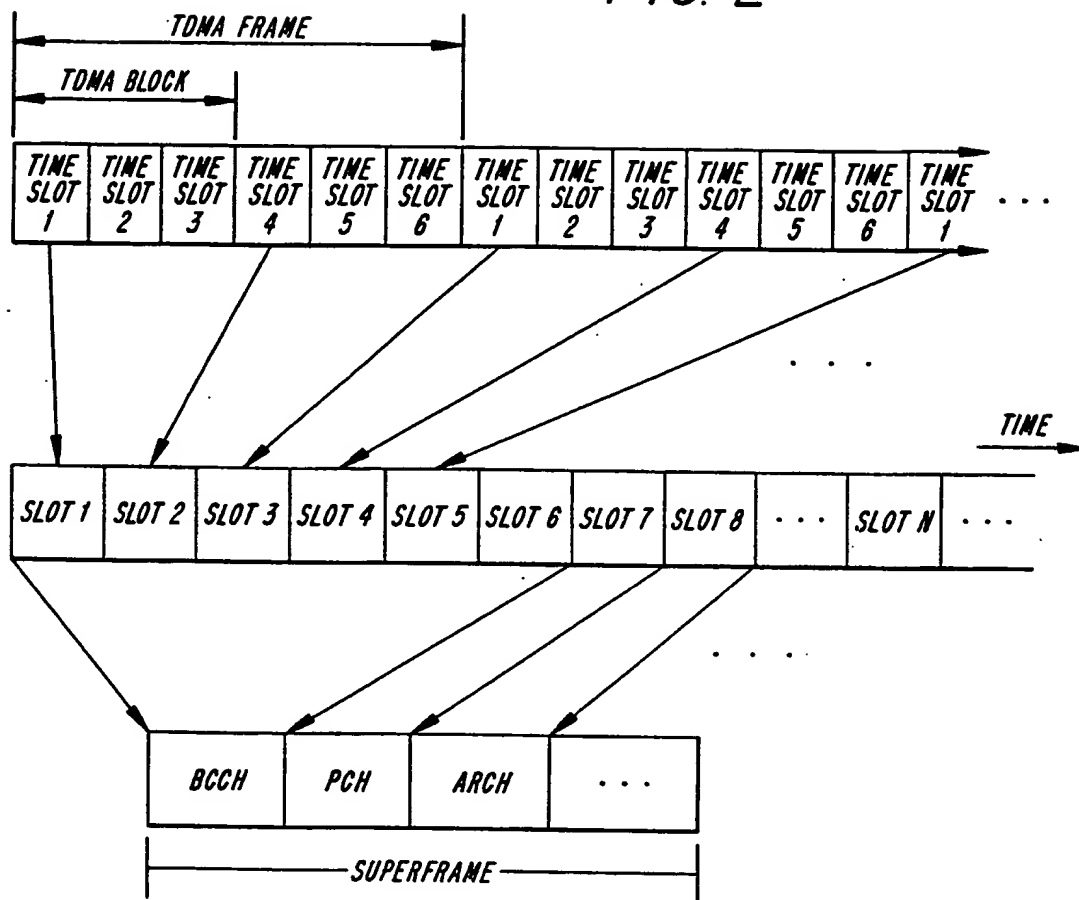
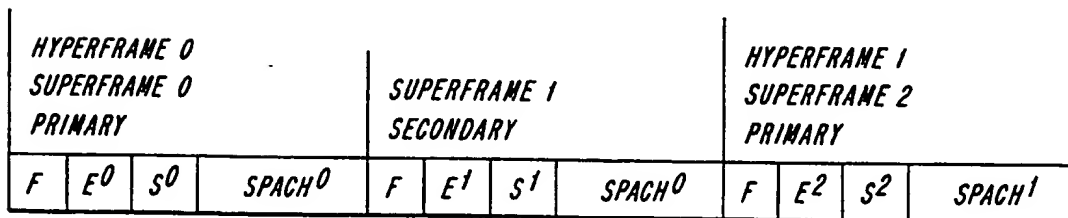
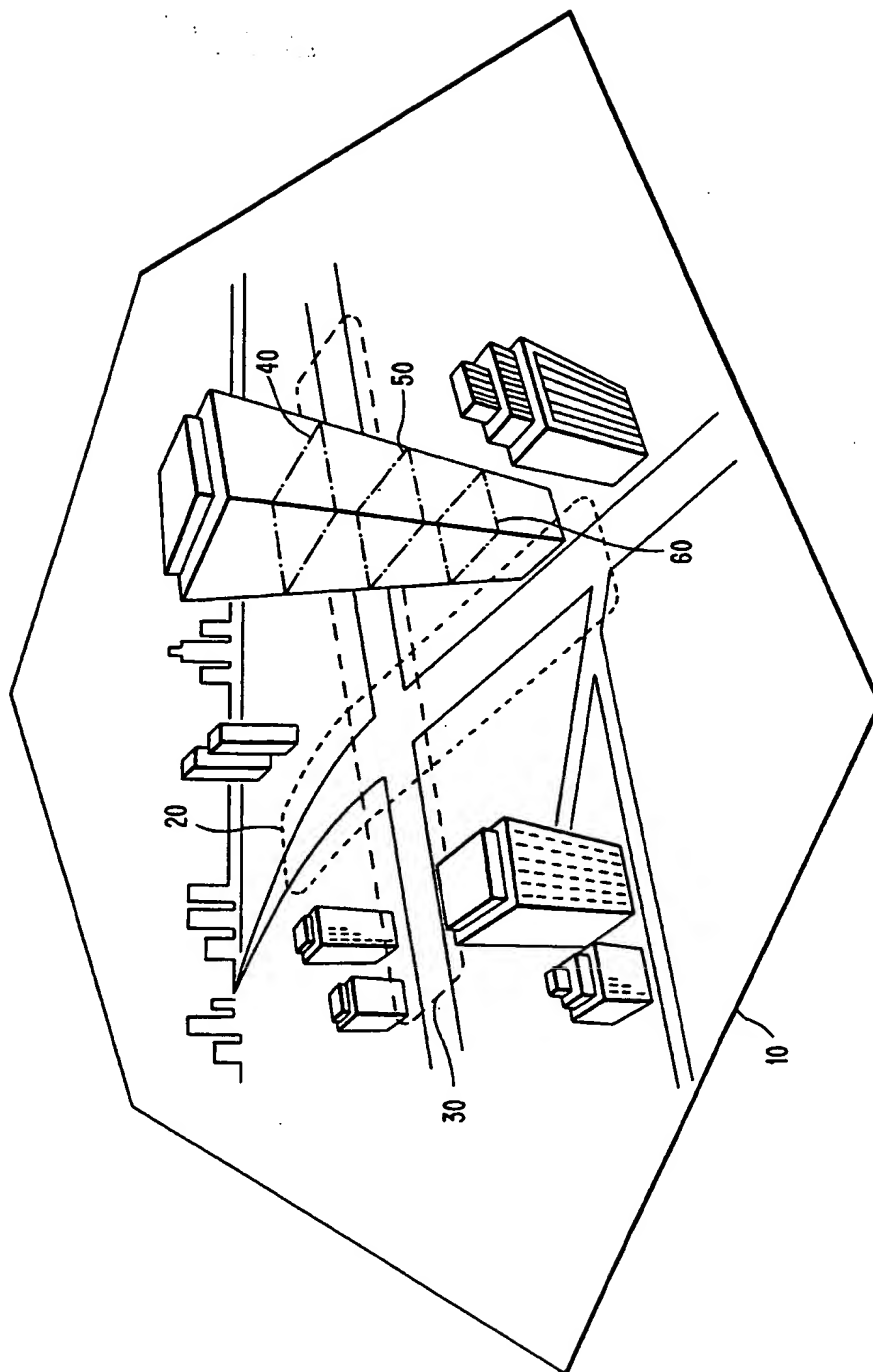


FIG. 5

**F** = F-BCCH**E** = E-BCCH**S** = S-BCCH**SPACH** = PCH OR ARCH OR SMSCH

THIS PAGE BLANK (USPTO)

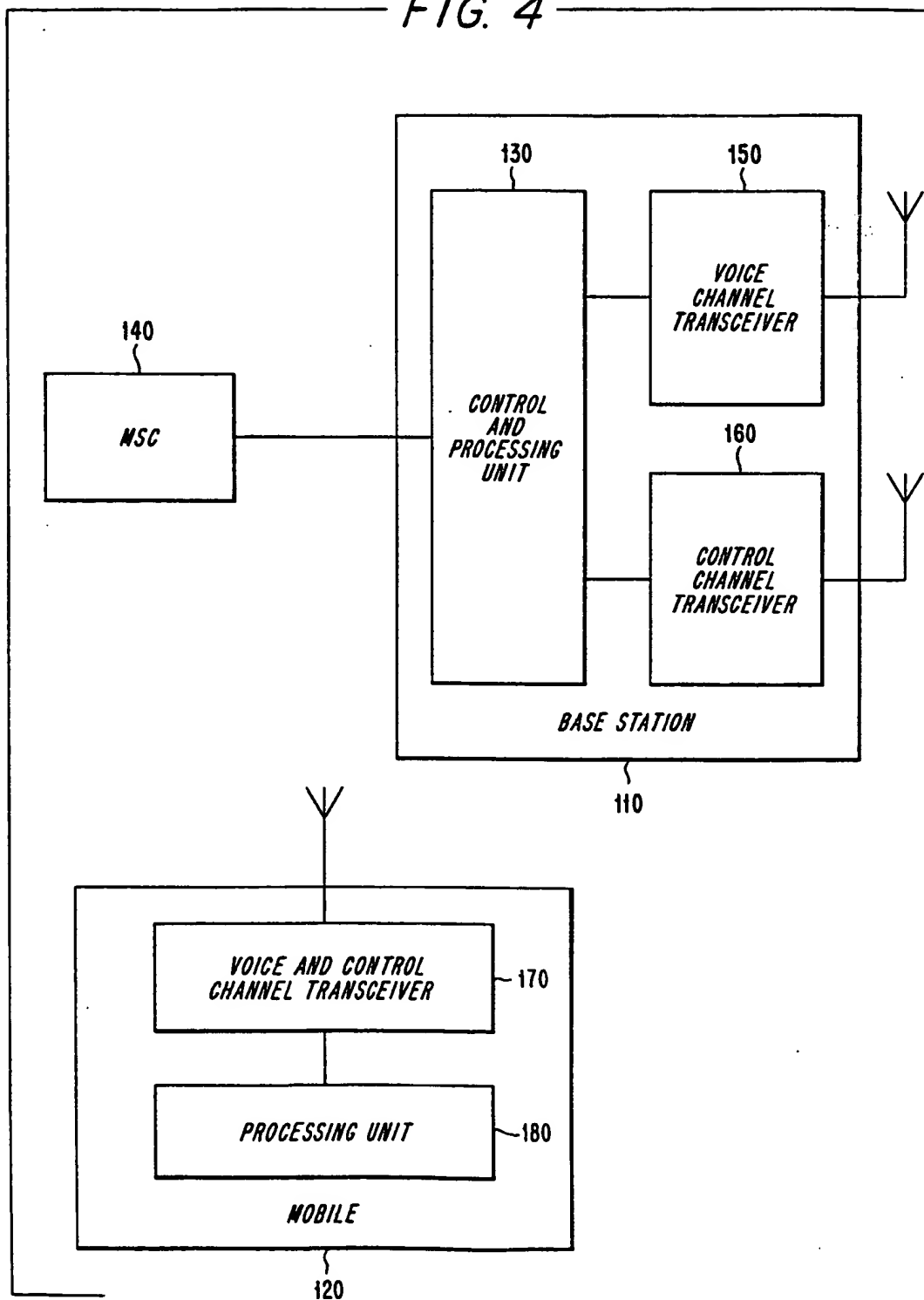
FIG. 3



THIS PAGE BLANK (USPTO)

4/10

FIG. 4



THIS PAGE BLANK (USPTO)

5/10

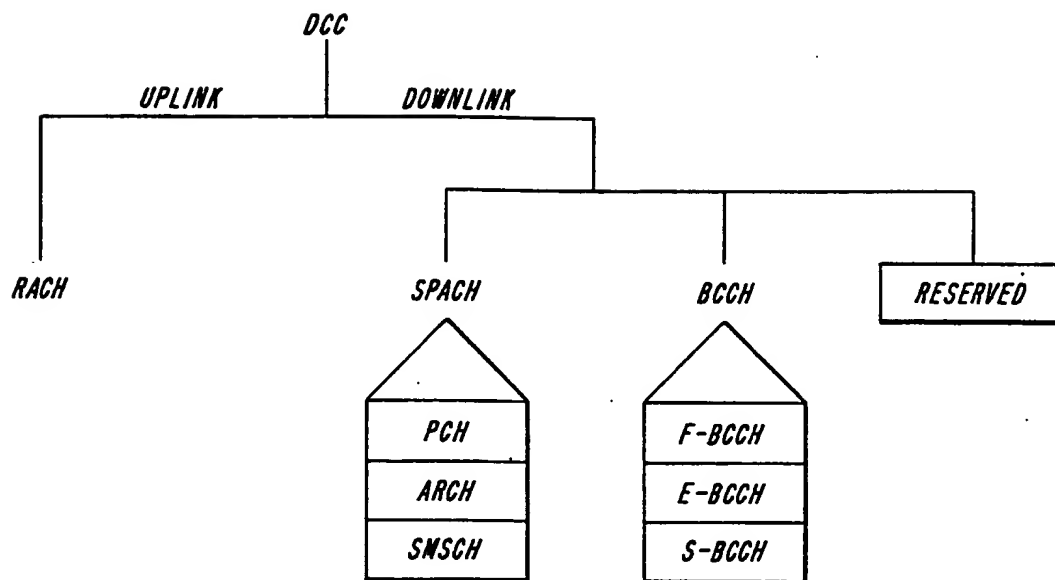


FIG. 6

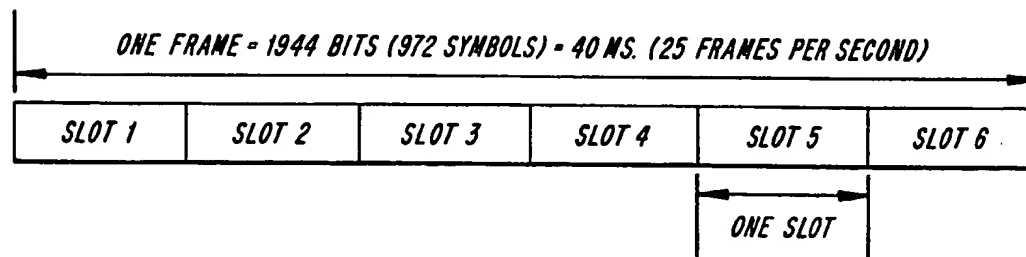


FIG. 7

THIS PAGE BLANK (USPTO)

6/10

FIG. 8a

6	6	16	28	122	24	122
6	R	PREAM	SYNC	DATA	SYNC+	DATA

FIG. 8b

6	6	16	28	122	24	78	44
6	R	PREAM	SYNC	DATA	SYNC+	DATA	AG

FIG. 8c

28	3	3	6	130	12	130	3	2	5	2
SYNC	BRI	R/N	CPE	DATA	CSFP	DATA	BRI	R/N	CPE	RSVD

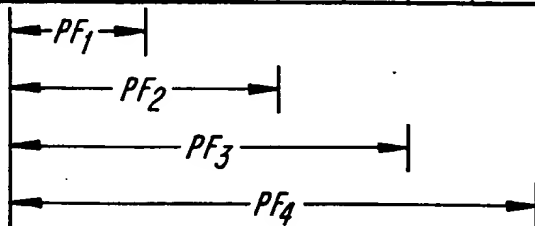
- AG* — ABBREVIATED GUARD TIME
- BRI* — BUSY/RESERVED/IDLE INDICATOR
- CSFP* — CODED SUPER FRAME PHASE
- DATA* — INFORMATION BITS
- 6* — GUARD TIME
- CPE* — CODED PARTIAL ECHO
- PREAM* — PREAMBLE
- R* — RAMP TIME
- R/N* — RECEIVED/NOT RECEIVED
- RSVD* — RESERVED FIELD, SET TO 11
- SYNC* — SYNCHRONIZATION
- SYNC+* — ADDITIONAL SYNCHRONIZATION

THIS PAGE BLANK (USPTO)

7/10

FIG. 10

HF_n	0		1		2		3		4		5		6	
SF_n	0	1	2	3	4	5	6	7	8	9	10	11	12	13
PF_1	p	s	p	s	p	s	p	s	p	s	p	s	p	s
PF_2	p	s	-	-	p	s	-	-	p	s	-	-	p	s
PF_3	p	s	-	-	-	-	p	s	-	-	-	-	p	s
PF_4	p	s	-	-	-	-	-	-	p	s	-	-	-	-

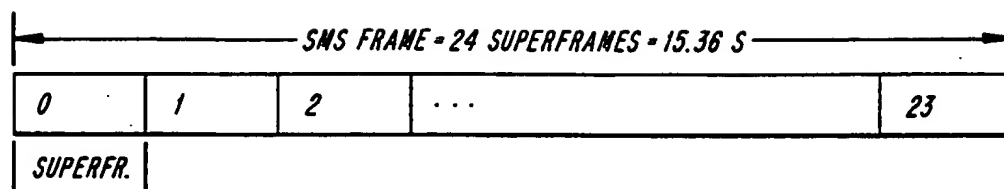
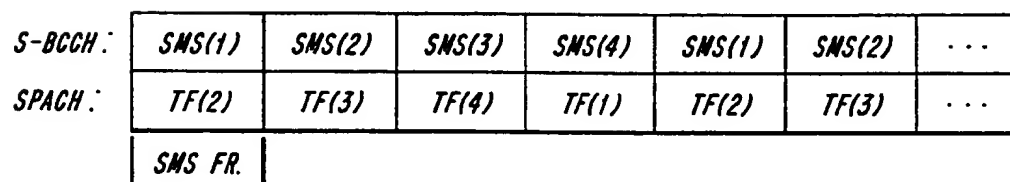


HF = HYPERFRAME
 SF = SUPERFRAME
 PF = PAGING FRAME
 P = PRIMARY PCHs
 S = SECONDARY PCHs

FIG. 9

109/101/79	16	5
INFORMATION	CRC	TAIL

THIS PAGE BLANK (USPTO)

*FIG. 11**FIG. 12*

THIS PAGE BLANK (USPTO)

FIG. 13a

SCS -X	BC -0	L3LI -X...X	L3DATA -X...X	BE -1	FILLER -0...0	CRC -X...X
1	1	8	8	1		16

FIG. 13b

SCS -X	BC -0	L3LI -X...X	L3DATA -X...X	BE -0	L3LI -X...X	L3DATA -X...X	CRC -X...X
1	1	8	8	1	8		16

FIG. 13c

SCS -X	BC -1	CLI -X...X	L3DATA -X...X	BE -1	FILLER -0...0	CRC -X...X
1	1	7	8	1		16

THIS PAGE BLANK (USPTO)

FIG. 14a

BC	SID	FDC	SSI	SCN	L3LI	L3DATA	CRC
-0	-7	-4	-1	-0	-X...X	-X...X	-X...X
1	5	8	1	1	8	85	16

FIG. 14b

BC	SID	FDC	SSI	SCN	CLI	L3DATA	BI	FILLER	CRC
-1	-7	-1	-0	-0	-X...X	-X...X	-0	-0...0	-X...X
1	5	8	1	1	7	1	1	16	

FIG. 14c

BC	SID	FDC	SSI	SCN	CLI	L3DATA	BI	L3LI	L3DATA	CRC
-1	-7	-3	-0	-0	-X...X	-X...X	-1	-X...X	-X...X	-X...X
1	5	8	1	1	7	1	1	8	16	

FIG. 14d

BC	SID	FDC	SSI	SCN	CLI	L3DATA	CRC
-1	-7	-2	-0	-0	-X...X	-X...X	-X...X
1	5	8	1	1	7	86	16

THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

Int ional Application No
PCT/SE 96/00716

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04Q7/38 H04B7/24

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04Q H04B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO,A,95 12931 (ERICSSON) 11 May 1995 cited in the application see page 41, line 1 - line 25; claims 1,3,11,13,14,27,28	1-10
X	WO,A,95 12936 (ERICSSON) 11 May 1995 see claims 41-52	7-10
X	US,A,5 267 175 (HOOPER) 30 November 1993 see column 3, line 18 - column 4, line 24	7-10



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search

18 October 1996

Date of mailing of the international search report

12.11.96

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax (+31-70) 340-3016

Authorized officer

Bischof, J-L

THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/SE 96/00716

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO-A-9512931	11-05-95	AU-A- 1048095	23-05-95
		AU-A- 1048395	23-05-95
		AU-A- 1087495	23-05-95
		AU-A- 1087695	23-05-95
		AU-A- 7757094	18-05-95
		AU-A- 8131394	23-05-95
		AU-A- 8131494	23-05-95
		BR-A- 9404316	04-07-95
		BR-A- 9405702	28-11-95
		BR-A- 9405703	28-11-95
		BR-A- 9405704	28-11-95
		BR-A- 9405705	28-11-95
		BR-A- 9405743	05-12-95
		BR-A- 9405927	05-12-95
		CA-A- 2134695	02-05-95
		CA-A- 2152942	11-05-95
		CA-A- 2152943	11-05-95
		CA-A- 2152944	11-05-95
		CA-A- 2152945	11-05-95
		CA-A- 2152946	11-05-95
		CA-A- 2152947	11-05-95
		CN-A- 1112345	22-11-95
		CN-A- 1117329	21-02-96
		CN-A- 1116888	14-02-96
		CN-A- 1117330	21-02-96
		CN-A- 1117331	21-02-96
		CN-A- 1124074	05-06-96
		CN-A- 1117332	21-02-96
		EP-A- 0652680	10-05-95
		EP-A- 0682829	22-11-95
		EP-A- 0679304	02-11-95
		EP-A- 0677222	18-10-95
		EP-A- 0681766	15-11-95
		EP-A- 0677223	18-10-95
		EP-A- 0677224	18-10-95
		FI-A- 953262	30-08-95
		FI-A- 953263	30-06-95
		FI-A- 953264	30-06-95
		FI-A- 953265	30-06-95
		FI-A- 953266	30-06-95

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/SE 96/00716

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO-A-9512931		FI-A- 953267	22-08-95
		FI-A- 953268	30-06-95
		JP-T- 8508627	10-09-96
		JP-T- 8508628	10-09-96
		JP-T- 8508629	10-09-96
		JP-T- 8508630	10-09-96
		JP-T- 8508631	10-09-96
		SE-A- 9403725	19-06-95
		WO-A- 9512933	11-05-95
		WO-A- 9512934	11-05-95

WO-A-9512936	11-05-95	AU-A- 1048095	23-05-95
		AU-A- 1048395	23-05-95
		AU-A- 1087495	23-05-95
		AU-A- 1087695	23-05-95
		AU-A- 7757094	18-05-95
		AU-A- 8131394	23-05-95
		AU-A- 8131494	23-05-95
		BR-A- 9404316	04-07-95
		BR-A- 9405702	28-11-95
		BR-A- 9405703	28-11-95
		BR-A- 9405704	28-11-95
		BR-A- 9405705	28-11-95
		BR-A- 9405743	05-12-95
		BR-A- 9405927	05-12-95
		CA-A- 2134695	02-05-95
		CA-A- 2152942	11-05-95
		CA-A- 2152943	11-05-95
		CA-A- 2152944	11-05-95
		CA-A- 2152945	11-05-95
		CA-A- 2152946	11-05-95
		CA-A- 2152947	11-05-95
		CN-A- 1112345	22-11-95
		CN-A- 1117329	21-02-96
		CN-A- 1116888	14-02-96
		CN-A- 1117330	21-02-96
		CN-A- 1117331	21-02-96
		CN-A- 1124074	05-06-96
		CN-A- 1117332	21-02-96
		EP-A- 0652680	10-05-95

THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/SE 96/00716

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO-A-9512936		EP-A- 0682829	22-11-95
		EP-A- 0679304	02-11-95
		EP-A- 0677222	18-10-95
		EP-A- 0681766	15-11-95
		EP-A- 0677223	18-10-95
		EP-A- 0677224	18-10-95
		FI-A- 953262	30-08-95
		FI-A- 953263	30-06-95
		FI-A- 953264	30-06-95
		FI-A- 953265	30-06-95
		FI-A- 953266	30-06-95
		FI-A- 953267	22-08-95
		FI-A- 953268	30-06-95
		JP-T- 8508627	10-09-96
		JP-T- 8508628	10-09-96
		JP-T- 8508629	10-09-96
		JP-T- 8508630	10-09-96
		JP-T- 8508631	10-09-96
		SE-A- 9403725	19-06-95
		WO-A- 9512933	11-05-95
		WO-A- 9512934	11-05-95
US-A-5267175	30-11-93	AU-A- 7728287	17-03-88
		EP-A- 0267379	18-05-88
		JP-A- 63153675	27-06-88

THIS PAGE BLANK (USPTO)